



VPN 3000 Concentrator Series User Guide

Release 2.5
July 2000

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7811137=
Text Part Number: 78-11137-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0005R)

VPN 3000 Concentrator Series User Guide
Copyright © 2000, Cisco Systems, Inc.
All rights reserved.



Preface

About this manual	xxxvii
Prerequisites	xxxvii
Organization	xxxvii
Additional Documentation	xxxviii
Other references	xxxix
Documentation Conventions	xxxix
Data Formats	xl
IP addresses	xl
Subnet masks and wildcard masks	xl
MAC addresses	xl
Hostnames	xl
Text strings	xl
Filenames	xl
Port numbers	xl
Contacting Cisco with questions	xli

1 Using the VPN 3000 Concentrator Series Manager

Browser requirements	1-1
JavaScript	1-1
Cookies	1-2
Navigation toolbar	1-2
Recommended PC monitor / display settings	1-2
Connecting to the VPN Concentrator using HTTP	1-3
Installing the SSL certificate in your browser	1-3
Installing the SSL certificate with Internet Explorer	1-4
Viewing certificates with Internet Explorer	1-9
Installing the SSL certificate with Netscape	1-10
Reinstallation	1-10
First-time installation	1-10
Viewing certificates with Netscape	1-15
Connecting to the VPN Concentrator using HTTPS	1-17
Logging in the VPN Concentrator Manager	1-18
Configuring HTTP, HTTPS, and SSL parameters	1-19
Understanding the VPN Concentrator Manager window	1-19
Title bar	1-19
Status bar	1-19
Mouse pointer and tips	1-20
Top frame (Manager toolbar)	1-20
Main tab	1-20
Help tab	1-20
Support tab	1-20

Logout tab	1-21
Logged in: [username]	1-21
Configuration tab	1-21
Administration tab	1-21
Monitoring tab	1-21
Save	1-21
Save Needed	1-21
Refresh	1-22
Cisco Systems logo	1-22
Left frame (Table of contents)	1-22
Main section titles (Configuration, Administration, Monitoring)	1-22
Closed or collapsed	1-22
Open or expanded	1-22
Main frame (Manager screen)	1-22
Organization of the VPN Concentrator Manager	1-23
Navigating the VPN Concentrator Manager	1-24

2 Configuration

Configuration	2-1
----------------------	------------

3 Interfaces

Configuration Interfaces	3-2
Interface	3-3
Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External)	3-4
WAN Interface in slot N, Port A B	3-4
Status	3-4
IP Address	3-4
Subnet Mask	3-4
Power Supplies	3-5
Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External) module in back-panel image	3-5
WAN Card Slot N module in back-panel image	3-5
Configuration Interfaces Power	3-5
Alarm Thresholds	3-6
CPU	3-6
Power Supply A, B	3-6
Board	3-6
Apply / Cancel	3-7
Configuration Interfaces Ethernet 1 2 3	3-7
Using the tabs	3-7
General Parameters tab	3-8
Enabled	3-8
IP Address	3-8
Subnet Mask	3-8
Public Interface	3-8
MAC Address	3-9
Filter	3-9
Speed	3-9
Duplex	3-9

RIP Parameters tab	3-10
Inbound RIP	3-10
Outbound RIP	3-10
OSPF Parameters tab	3-11
OSPF Enabled	3-11
OSPF Area ID	3-11
OSPF Priority	3-12
OSPF Metric	3-12
OSPF Retransmit Interval	3-12
OSPF Hello Interval	3-12
OSPF Dead Interval	3-12
OSPF Transit Delay	3-12
OSPF Authentication	3-13
OSPF Password	3-13
Apply / Cancel	3-13
Configuration Interfaces WAN Card in Slot N	3-14
Interface	3-14
Status	3-14
IP Address	3-15
Subnet Mask	3-15
Configuration Interfaces WAN Card in Slot N Port A B Select T1/E1	3-15
T1: up to 24 64-Kbps channels	3-15
E1: up to 31 64-Kbps channels	3-16
Configuration Interfaces WAN Card in Slot N Port A B as T1 or E1	3-16
Using the tabs	3-16
IP Parameters tab	3-17
Enabled	3-17
IP Address	3-17
Subnet Mask	3-17
Public Interface	3-17
Filter	3-18
RIP Parameters tab	3-18
Inbound RIP	3-19
Outbound RIP	3-19
OSPF Parameters tab	3-20
OSPF Enabled	3-20
OSPF Area ID	3-20
OSPF Priority	3-21
OSPF Metric	3-21
OSPF Retransmit Interval	3-21
OSPF Hello Interval	3-21
OSPF Dead Interval	3-21
OSPF Transit Delay	3-21
OSPF Authentication	3-22
OSPF Password	3-22
WAN Parameters tab	3-23
Line Coding	3-23
Line Framing	3-23
T1 selections:	3-23
E1 selections:	3-23
Buildout	3-24
Clock Source	3-24
Data Inversion	3-24

Loopback	3-24
Timeslots	3-24
PPP Multilink Parameters tab	3-25
Enable PPP Multilink	3-25
Apply / Cancel	3-25

4 System Configuration

Configuration System	4-1
-------------------------------------	-----

5 Servers

Configuration System Servers	5-1
Configuration System Servers Authentication	5-2
Authentication Servers	5-3
Add / Modify / Delete / Move / Test	5-3
Configuration System Servers Authentication Add or Modify	5-3
Server Type = RADIUS	5-4
Authentication Server	5-4
Server Port	5-4
Timeout	5-4
Retries	5-4
Server Secret	5-5
Verify	5-5
Add or Apply / Cancel	5-5
Server Type = NT Domain	5-5
Authentication Server Address	5-5
Server Port	5-6
Timeout	5-6
Retries	5-6
Domain Controller Name	5-6
Add or Apply / Cancel	5-6
Server Type = SDI	5-6
Authentication Server	5-7
Server Port	5-7
Timeout	5-7
Retries	5-7
Add or Apply / Cancel	5-7
Server Type = Internal Server	5-8
Add / Cancel	5-8
Configuration System Servers Authentication Delete	5-8
Yes / No	5-9
Configuration System Servers Authentication Test	5-9
User Name	5-9
Password	5-9
OK / Cancel	5-9
Authentication Server Test: Success	5-10
Continue	5-10
Authentication Server Test: Authentication Rejected Error	5-10
Authentication Server Test: Authentication Error	5-10

Configuration System Servers Accounting	5-11
Accounting Servers	5-12
Add / Modify / Delete / Move	5-12
Configuration System Servers Accounting Add or Modify	5-13
Accounting Server	5-13
Server Port	5-13
Timeout	5-13
Retries	5-14
Server Secret	5-14
Verify	5-14
Add or Apply / Cancel	5-14
Configuration System Servers DNS	5-14
Enabled	5-15
Domain	5-15
Primary DNS Server	5-15
Secondary DNS Server	5-15
Tertiary DNS Server	5-15
Timeout Period	5-16
Timeout Retries	5-16
Apply / Cancel	5-16
Configuration System Servers DHCP	5-16
DHCP Servers	5-17
Add / Modify / Delete / Move	5-17
Configuration System Servers DHCP Add or Modify	5-18
DHCP Server	5-18
Server Port	5-18
Add or Apply / Cancel	5-18
Configuration System Servers NTP	5-18
Configuration System Servers NTP Parameters	5-19
Sync Frequency	5-19
Apply / Cancel	5-19
Configuration System Servers NTP Hosts	5-20
NTP Hosts	5-20
Add / Modify / Delete	5-20
Configuration System Servers NTP Hosts Add or Modify	5-21
NTP Host	5-21
Add or Apply / Cancel	5-21

6 Address Management

Configuration System Address Management	6-1
Configuration System Address Management Assignment	6-2
Use Client Address	6-2
Use Address from Authentication Server	6-2
Use DHCP	6-2
Use Address Pools	6-3
Apply / Cancel	6-3
Configuration System Address Management Pools	6-3
IP Pool Entry	6-3
Add / Modify / Delete	6-4

Configuration System Address Management Pools Add or Modify	6-4
Range Start	6-4
Range End	6-4
Add or Apply / Cancel	6-5

7 Tunneling Protocols

Configuration System Tunneling Protocols	7-2
Configuration System Tunneling Protocols PPTP	7-2
Enabled	7-3
Maximum Tunnel Idle Time	7-3
Packet Window Size	7-4
Limit Transmit to Window	7-4
Max. Tunnels	7-4
Max. Sessions/Tunnel	7-4
Packet Processing Delay	7-4
Acknowledgement Delay	7-4
Acknowledgement Timeout	7-4
Apply / Cancel	7-5
Configuration System Tunneling Protocols L2TP	7-5
Enabled	7-6
Maximum Tunnel Idle Time	7-6
Control Window Size	7-6
Control Retransmit Interval	7-6
Control Retransmit Limit	7-6
Max. Tunnels	7-6
Max. Sessions/Tunnel	7-6
Hello Interval	7-7
Apply / Cancel	7-7
Configuration System Tunneling Protocols IPSec	7-7
Configuration System Tunneling Protocols IPSec LAN-to-LAN	7-8
LAN-to-LAN Connection	7-9
Add / Modify / Delete	7-9
Configuration System Tunneling Protocols IPSec LAN-to-LAN No Public Interfaces	7-10
Configuration System Tunneling Protocols IPSec LAN-to-LAN Add or Modify	7-10
Name	7-12
Interface	7-12
Peer	7-12
Digital Certificate	7-13
Preshared Key	7-13
Authentication	7-13
Encryption	7-13
IKE Proposal	7-14
Network Autodiscovery	7-14
Local Network	7-14
Network List	7-14
IP Address	7-15
Wildcard Mask	7-15

Remote Network	7-15
Network List	7-15
IP Address	7-15
Wildcard Mask	7-16
Add or Apply / Cancel	7-16
Configuration System Tunneling Protocols IPSec LAN-to-LAN Add 	
Local or Remote Network List	7-16
List Name	7-17
Network List	7-17
Generate Local List	7-18
Add	7-18
Configuration System Tunneling Protocols IPSec LAN-to-LAN Add Done	7-18
OK	7-19
Configuration System Tunneling Protocols IPSec IKE Proposals	7-19
Active Proposals	7-21
Inactive Proposals	7-21
<< Activate	7-21
>> Deactivate	7-21
Move Up / Move Down	7-21
Add	7-21
Modify	7-22
Copy	7-22
Delete	7-22
Configuration System Tunneling Protocols IPSec IKE Proposals Add, Modify, or Copy	7-22
Proposal Name	7-23
Authentication Mode	7-23
Authentication Algorithm	7-24
Encryption Algorithm	7-24
Diffie-Hellman Group	7-24
Lifetime Measurement	7-24
Data Lifetime	7-25
Time Lifetime	7-25
Add or Apply / Cancel	7-25

8 IP Routing

Configuration System IP Routing	8-2
Configuration System IP Routing Static Routes	8-2
Static Routes	8-3
Add / Modify / Delete	8-3
Configuration System IP Routing Static Routes Add or Modify	8-3
Network Address	8-4
Subnet Mask	8-4
Metric	8-4
Destination	8-4
Router Address	8-4
Interface	8-4
Add or Apply / Cancel	8-4
Configuration System IP Routing Default Gateways	8-5
Default Gateway	8-5
Metric	8-5

Tunnel Default Gateway	8-6
Override Default Gateway	8-6
Apply / Cancel	8-6
Configuration System IP Routing OSPF	8-6
Enabled	8-7
Router ID	8-7
Autonomous System	8-7
Apply / Cancel	8-8
Configuration System IP Routing OSPF Areas	8-8
OSPF Area	8-8
Add / Modify / Delete	8-8
Configuration System IP Routing OSPF Areas Add or Modify	8-9
Area ID	8-9
Area Summary	8-9
External LSA Import	8-10
Add or Apply / Cancel	8-10
Configuration System IP Routing DHCP	8-10
Enabled	8-10
Lease Timeout	8-11
Listen Port	8-11
Timeout Period	8-11
Apply / Cancel	8-11
Configuration System IP Routing Redundancy	8-12
Enable VRRP	8-13
Group ID	8-13
Group Password	8-13
Role	8-13
Advertisement Interval	8-13
Group Shared Addresses	8-13
1 (Private)	8-13
2 (Public)	8-14
3 (External)	8-14
Apply / Cancel	8-14

9 Management Protocols

Configuration System Management Protocols	9-1
Configuration System Management Protocols FTP	9-2
Enable	9-2
Port	9-2
Maximum Connections	9-2
Apply / Cancel	9-2
Configuration System Management Protocols HTTP/HTTPS	9-3
Enable HTTP	9-3
Enable HTTPS	9-4
HTTP Port	9-4
HTTPS Port	9-4
Maximum Sessions	9-4
Apply / Cancel	9-4
Configuration System Management Protocols TFTP	9-4
Enable	9-5

Port	9-5
Maximum Connections	9-5
Timeout	9-5
Apply / Cancel	9-5
Configuration System Management Protocols Telnet	9-6
Enable Telnet	9-6
Enable Telnet/SSL	9-6
Telnet Port	9-6
Telnet/SSL Port	9-7
Maximum Connections	9-7
Apply / Cancel	9-7
Configuration System Management Protocols SNMP	9-7
Enable	9-8
Port	9-8
Maximum Queued Requests	9-8
Apply / Cancel	9-8
Configuration System Management Protocols SNMP Communities	9-8
Community Strings	9-9
Add / Modify / Delete	9-9
Configuration System Management Protocols SNMP Communities Add or Modify	9-10
Community String	9-10
Add or Apply / Cancel	9-10
Configuration System Management Protocols SSL	9-10
Encryption Protocols	9-12
Client Authentication	9-12
SSL Version	9-12
Generated Certificate Key Size	9-13
Apply / Cancel	9-13

10 Events

Event class	10-1
Event severity level	10-4
Event log	10-5
Event log data	10-5
Configuration System Events	10-5
Configuration System Events General	10-6
Save Log on Wrap	10-6
Save Log Format	10-7
FTP Saved Log on Wrap	10-7
Email Source Address	10-7
Syslog Format	10-7
Severity to Log	10-7
Severity to Console	10-8
Severity to Syslog	10-8
Severity to Email	10-8
Severity to Trap	10-8
Apply / Cancel	10-9

Configuration System Events FTP Backup	10-9
FTP Server	10-9
FTP Directory	10-9
FTP Username	10-9
FTP Password	10-9
Verify	10-10
Apply / Cancel	10-10
Configuration System Events Classes	10-10
Configured Event Classes	10-10
Add / Modify / Delete	10-11
Configuration System Events Classes Add or Modify	10-11
Class Name	10-12
Enable	10-12
Severity to Log	10-12
Severity to Console	10-12
Severity to Syslog	10-12
Severity to Email	10-13
Severity to Trap	10-13
Add or Apply / Cancel	10-13
Configuration System Events Trap Destinations	10-14
Trap Destinations	10-14
Add / Modify / Delete	10-14
Configuration System Events Trap Destinations Add or Modify	10-15
Destination	10-15
SNMP Version	10-15
Community	10-15
Port	10-16
Add or Apply / Cancel	10-16
Configuration System Events Syslog Servers	10-16
Syslog Servers	10-17
Add / Modify / Delete	10-17
Configuration System Events Syslog Servers Add or Modify	10-17
Syslog Server	10-17
Port	10-18
Facility	10-18
Add or Apply / Cancel	10-18
Configuration System Events SMTP Servers	10-18
SMTP Servers	10-19
Add / Modify / Delete / Move	10-19
Configuration System Events SMTP Servers Add or Modify	10-20
SMTP Server	10-20
Add or Apply / Cancel	10-20
Configuration System Events Email Recipients	10-20
Email Recipients	10-21
Add / Modify / Delete	10-21
Configuration System Events Email Recipients Add or Modify	10-22
Email Address	10-22
Max Severity	10-22
Add or Apply / Cancel	10-23

11 General

Configuration System General	11-1
Configuration System General Identification	11-2
System Name	11-2
Contact	11-2
Location	11-2
Apply / Cancel	11-2
Configuration System General Time and Date	11-3
Current Time	11-3
New Time	11-3
Enable DST Support	11-3
Apply / Cancel	11-3

12 User Management

Configuration User Management	12-3
Configuration User Management Base Group	12-3
Using the tabs	12-3
General Parameters tab	12-4
Access Hours	12-4
Simultaneous Logins	12-5
Minimum Password Length	12-5
Allow Alphabetic-Only Passwords	12-5
Idle Timeout	12-5
Maximum Connect Time	12-5
Filter	12-5
Primary DNS	12-6
Secondary DNS	12-6
Primary WINS	12-6
Secondary WINS	12-6
SEP Card Assignment	12-6
Tunneling Protocols	12-6
IPSec Parameters tab	12-7
IPSec SA	12-7
Tunnel Type	12-8
<i>Remote Access Parameters</i>	12-8
Group Lock	12-8
Authentication	12-9
Mode Configuration	12-9
<i>Mode Configuration Parameters</i>	12-9
Banner	12-9
Allow Password Storage on Client	12-10
Split Tunneling Network List	12-10
Default Domain Name	12-11
IPSec through NAT	12-11
IPSec through NAT UDP Port	12-11
PPTP/L2TP Parameters tab	12-12
Use Client Address	12-12
PPTP Authentication Protocols	12-12
PPTP Encryption	12-13
L2TP Authentication Protocols	12-14
L2TP Encryption	12-14
Apply / Cancel	12-15

Configuration User Management Groups	12-16
Current Groups	12-16
Add / Modify / Delete	12-17
Configuration User Management Groups Add or Modify (Internal)	12-18
Using the tabs	12-18
Identity Parameters tab	12-18
Group Name	12-19
Password	12-19
Verify	12-19
Type	12-19
General Parameters tab	12-20
Value / Inherit?	12-20
Access Hours	12-21
Simultaneous Logins	12-21
Minimum Password Length	12-21
Allow Alphabetic-Only Passwords	12-21
Idle Timeout	12-21
Maximum Connect Time	12-22
Filter	12-22
Primary DNS	12-22
Secondary DNS	12-22
Primary WINS	12-23
Secondary WINS	12-23
SEP Card Assignment	12-23
Tunneling Protocols	12-23
IPSec Parameters tab	12-24
Value / Inherit?	12-25
IPSec SA	12-25
Tunnel Type	12-26
<i>Remote Access Parameters</i>	12-26
Group Lock	12-26
Authentication	12-26
Mode Configuration	12-26
<i>Mode Configuration Parameters</i>	12-27
Banner	12-27
Allow Password Storage on Client	12-27
Split Tunneling Network List	12-27
Default Domain Name	12-27
IPSec through NAT	12-28
IPSec through NAT UDP Port	12-28
PPTP/L2TP Parameters tab	12-28
Value / Inherit?	12-29
Use Client Address	12-29
PPTP Authentication Protocols	12-29
PPTP Encryption	12-30
L2TP Authentication Protocols	12-30
L2TP Encryption	12-31
Add or Apply / Cancel	12-31

Configuration User Management Groups Modify (External)	12-32
Group Name	12-32
Password	12-32
Verify	12-32
Type	12-32
Apply / Cancel	12-33
Configuration User Management Users	12-33
Current Users	12-34
Add / Modify / Delete	12-34
Configuration User Management Users Add or Modify	12-34
Using the tabs	12-34
Identity Parameters tab	12-35
User Name	12-35
Password	12-35
Verify	12-35
Group	12-35
IP Address	12-36
Subnet Mask	12-36
General Parameters tab	12-36
Value / Inherit?	12-37
Access Hours	12-37
Simultaneous Logins	12-37
Idle Timeout	12-37
Maximum Connect Time	12-38
Filter	12-38
SEP Card Assignment	12-38
Tunneling Protocols	12-38
IPSec Parameters tab	12-39
Value / Inherit?	12-39
IPSec SA	12-40
Store Password on Client	12-40
PPTP/L2TP Parameters tab	12-41
Value / Inherit?	12-41
Use Client Address	12-42
PPTP Authentication Protocols	12-42
L2TP Authentication Protocols	12-43
Add or Apply / Cancel	12-43

13 Policy Management

Configuration Policy Management	13-2
Configuration Policy Management Access Hours	13-2
Current Access Hours	13-3
Add / Modify / Delete	13-3
Configuration Policy Management Access Hours Add or Modify	13-4
Name	13-4
Sunday - Saturday	13-4
Add or Apply / Cancel	13-5
Configuration Policy Management Traffic Management	13-5
Configuration Policy Management Traffic Management Network Lists	13-6
Network List	13-6
Add / Modify / Copy / Delete	13-6

Configuration Policy Management Traffic Management Network Lists Add, Modify, or Copy	13-7
List Name	13-8
Network List	13-8
Generate Local List	13-8
Add or Apply / Cancel	13-8
Configuration Policy Management Traffic Management Rules	13-9
Filter Rules	13-9
Add / Modify / Copy / Delete	13-11
Configuration Policy Management Traffic Management Rules Add, Modify, or Copy	13-12
Rule Name	13-14
Direction	13-14
Action	13-14
Protocol or Other	13-14
TCP Connection	13-15
Source Address	13-15
Network List	13-15
IP Address	13-16
Wildcard-mask	13-16
Destination Address	13-16
Network List	13-16
IP Address	13-16
Wildcard-mask	13-16
TCP/UDP Source Port	13-16
Port or Range	13-17
TCP/UDP Destination Port	13-18
Port or Range	13-18
ICMP Packet Type	13-18
Add or Apply / Cancel	13-18
Configuration Policy Management Traffic Management Rules Delete	13-19
Yes / No	13-19
Configuration Policy Management Traffic Management Security Associations	13-19
IPSec SAs	13-21
Add / Modify / Delete	13-21
Configuration Policy Management Traffic Management Security Associations Add or Modify	13-22
SA Name	13-23
Inheritance	13-23
<i>IPSec Parameters</i>	<i>13-24</i>
Authentication Algorithm	13-24
Encryption Algorithm	13-24
Encapsulation Mode	13-24
Perfect Forward Secrecy	13-25
Lifetime Measurement	13-25
Data Lifetime	13-25
Time Lifetime	13-25
<i>IKE Parameters</i>	<i>13-26</i>
IKE Peer	13-26
Negotiation Mode	13-26
Digital Certificate	13-26
IKE Proposal	13-27
Add or Apply / Cancel	13-27
Configuration Policy Management Traffic Management Security Associations Delete	13-28
Yes / No	13-28

Configuration Policy Management Traffic Management Filters	13-28
Filter List	13-30
Add Filter	13-30
Assign Rules to Filter	13-30
Modify Filter	13-30
Copy Filter	13-31
Delete Filter	13-31
Configuration Policy Management Traffic Management Filters Add, Modify, or Copy	13-31
Filter Name	13-32
Default Action	13-32
Source Routing	13-33
Fragments	13-33
Description	13-33
Add or Apply / Cancel	13-33
Configuration Policy Management Traffic Management Assign Rules to Filter	13-34
Filter Name:	13-34
Current Rules in Filter	13-35
Available Rules	13-35
<< Add	13-35
<< Insert Above	13-35
>> Remove	13-35
Move Up / Move Down	13-36
Assign SA to Rule	13-36
Done	13-36
Configuration Policy Management Traffic Management Assign Rules to Filter Add SA to Rule ...	13-36
Add SA to Rule on Filter:	13-37
IPSec SAs	13-37
Apply	13-37
Configuration Policy Management Traffic Management Assign Rules to Filter Change SA on Rule	13-37
Change SA on Rule in Filter:	13-38
IPSec SAs	13-38
Apply / Cancel	13-38
Configuration Policy Management Traffic Management NAT	13-39
Configuration Policy Management Traffic Management NAT Enable	13-40
Enabled	13-40
Apply / Cancel	13-40
Configuration Policy Management Traffic Management NAT Rules	13-40
NAT Rules	13-41
Add / Modify / Delete	13-41
Configuration Policy Management Traffic Management NAT Rules No Public Interfaces	13-42
Configuration Policy Management Traffic Management NAT Rules Add or Modify	13-42
Interface	13-43
Private Address	13-43
IP Address	13-43
Subnet Mask	13-43
Action	13-44
Add or Apply / Cancel	13-44

14 Administration

Administration	14-1
Administration Sessions	14-3
Refresh	14-3
Logout All: PPTP L2TP IPSec User L2TP/IPSec IPSec/NAT IPSec/LAN-to-LAN	14-4
Session Summary table	14-4
Active LAN-to-LAN Sessions	14-4
Active Remote Access Sessions	14-4
Active Management Sessions	14-4
Total Active Sessions	14-5
Peak Concurrent Sessions	14-5
Concurrent Sessions Limit	14-5
Total Cumulative Sessions	14-5
LAN-to-LAN Sessions table	14-5
[Remote Access Sessions Management Sessions]	14-5
Connection Name	14-5
IP Address	14-5
Protocol, Encryption, Login Time, Duration, Actions	14-5
Remote Access Sessions table	14-6
[LAN-to-LAN Sessions Management Sessions]	14-6
Username	14-6
Public IP Address	14-6
Assigned IP Address	14-6
Protocol, Encryption, Login Time, Duration, Actions	14-6
Management Sessions table	14-6
[LAN-to-LAN Sessions Remote Access Sessions]	14-6
Administrator	14-6
IP Address	14-7
Protocol, Encryption, Login Time, Duration, Actions	14-7
Configuration locked by	14-7
Administration Sessions Detail	14-8
Refresh	14-12
Back to Sessions	14-12
Administration Sessions Detail parameters	14-12
Administration Software Update	14-14
Current Software Revision	14-14
Browse...	14-15
Upload	14-15
Software Update Progress	14-15
Software Update Success	14-16
Software Update Error	14-16
Administration System Reboot	14-17
Action	14-18
Configuration	14-18
When to Reboot/Shutdown	14-18
Apply / Cancel	14-18
Administration Ping	14-19
Address/Hostname to Ping	14-19
Ping / Cancel	14-19
Success (Ping)	14-19
Continue	14-19
Error (Ping)	14-20

Administration Monitoring Refresh	14-20
Enable	14-20
Refresh Period	14-20
Apply / Cancel	14-21
Administration Access Rights	14-21
Administration Access Rights Administrators	14-21
Group Number	14-22
Username	14-22
Properties / Modify	14-22
Administrator	14-23
Enabled	14-23
Apply / Cancel	14-23
Administration Access Rights Administrators Modify Properties	14-23
Username	14-24
Password	14-24
Verify	14-24
Access Rights	14-24
Authentication	14-25
General	14-25
SNMP	14-25
Files	14-25
Apply / Default / Cancel	14-25
Administration Access Rights Access Control List	14-26
Manager Workstations	14-26
Add / Modify / Delete / Move	14-26
Administration Access Rights Access Control List Add or Modify	14-27
Priority (Modify screen only)	14-27
IP Address	14-27
IP Mask	14-28
Access Group	14-28
Add or Apply / Cancel	14-28
Administration Access Rights Access Settings	14-28
Session Idle Timeout	14-28
Session Limit	14-29
Encrypt Config File	14-29
Apply / Cancel	14-29
Administration File Management	14-29
Administration File Management Files	14-30
Refresh	14-30
Total, Used, Free KB	14-30
Filename	14-30
Size (bytes)	14-30
Date/Time	14-30
Actions	14-31
View (Save)	14-31
Delete	14-31
Copy	14-31
Administration File Management Swap Configuration Files	14-32
OK / Cancel	14-32

Administration File Management TFTP Transfer	14-32
Concentrator File	14-33
Action	14-33
TFTP Server	14-33
TFTP Server File	14-33
OK / Cancel	14-33
Success (TFTP)	14-34
Continue	14-34
Error (TFTP)	14-34
Administration Certificate Management	14-34
Installing digital certificates on the VPN Concentrator	14-36
Administration Certificate Management Enrollment	14-36
Common Name (CN)	14-37
Organizational Unit (OU)	14-37
Organization (O)	14-37
Locality (L)	14-38
State/Province (SP)	14-38
Country (C)	14-38
Subject Alternative Name (Fully Qualified Domain Name)	14-38
Key Size	14-38
Apply / Cancel	14-38
Administration Certificate Management Enrollment Request Generated	14-39
Enrolling with a Certificate Authority	14-40
Administration Certificate Management Installation	14-40
Certificate Type	14-41
Certificate Password	14-41
Verify	14-41
Local File / Browse	14-42
Apply / Cancel	14-42
Administration Certificate Management Certificates	14-42
Certificate Authorities	14-42
Identity Certificates	14-42
SSL Certificate / [Generate]	14-43
Subject / Issuer	14-43
Expiration	14-43
Actions / View / CRL / Delete	14-43
Administration Certificate Management Certificates View	14-44
Subject	14-44
Issuer	14-44
CN=	14-44
OU=	14-45
O=	14-45
L=	14-45
SP=	14-45
C=	14-45
Serial Number	14-45
Signing Algorithm	14-45
Public Key Type	14-45
Certificate Usage	14-45
MD5 Thumbprint	14-46
SHA1 Thumbprint	14-46
Validity	14-46

Subject Alternative Name (Fully Qualified Domain Name)	14-46
CRL Distribution Point	14-46
Back	14-46
Administration Certificate Management Certificates CRL	14-46
Certificate	14-47
Enable CRL Checking	14-47
Server	14-47
Server Port	14-48
Update Period	14-48
Filter	14-48
Base DN	14-48
Login DN	14-48
Password	14-48
Verify	14-48
Apply / Cancel	14-48
Administration Certificate Management Certificates Delete	14-49
Yes / No	14-49

15 Monitoring

Monitor	15-1
Monitor Routing Table	15-2
Refresh	15-2
Valid Routes	15-3
Address	15-3
Mask	15-3
Next Hop	15-3
Interface	15-3
Protocol	15-3
Age	15-4
Metric	15-4
Monitor Event Log	15-4
Select Filter Options	15-5
Event Class	15-5
Severities	15-5
Client IP Address	15-5
Events/Page	15-5
Direction	15-5
First Page	15-6
Previous Page	15-6
Next Page	15-6
Last Page	15-6
Get Log	15-6
Save Log	15-6
Clear Log	15-7
Event log format	15-7
Event sequence	15-7
Event date	15-7
Event time	15-7
Event severity	15-7
Event class / number	15-8
Event repeat	15-8

Event IP address	15-8
Event string	15-8
Monitor System Status	15-9
Refresh	15-10
VPN Concentrator Type	15-10
Bootcode Rev	15-10
Software Rev	15-10
Up Since	15-10
RAM Size	15-10
Front Panel	15-10
Back Panel	15-10
Fan 1, Fan 2	15-11
CPU, Cage	15-11
CPU Utilization	15-11
Active Sessions	15-11
Throughput	15-11
Monitor System Status Ethernet Interface	15-12
Refresh	15-12
Back	15-12
Interface	15-12
IP Address	15-12
Status	15-12
Rx Unicast	15-13
Tx Unicast	15-13
Rx Multicast	15-13
Tx Multicast	15-13
Rx Broadcast	15-13
Tx Broadcast	15-13
Monitor System Status Dual T1/E1 WAN Slot N	15-14
Refresh	15-14
Back	15-14
T1/E1 Statistics	15-14
Slot	15-14
Port	15-15
Status	15-15
Up Time Seconds	15-15
Errored Seconds	15-15
Severely Errored Seconds	15-15
Bursty Errored Seconds	15-15
Severely Errored Framing Seconds	15-16
Unavailable Seconds	15-16
Line Errored Seconds	15-16
Degraded Minutes	15-16
Bipolar Violations	15-16
Line Coding Violations	15-16
Path Coding Violations	15-16
Controlled Slips	15-16
Synchronous Statistics	15-16
Slot	15-17
Port	15-17
IfIndex	15-17
Status	15-17
Protocol	15-17

Packets Received	15-17
Bytes Received	15-17
Packets Transmitted	15-17
Bytes Transmitted	15-17
Received Frame Too Long	15-18
Transmit Frame Too Long	15-18
Received Byte Align Errors	15-18
Received CRC Errors	15-18
Receiver Overrun Errors	15-18
Transmits Dropped	15-18
Transmit Underruns	15-18
Monitor System Status Power	15-19
Refresh	15-19
Back	15-19
CPU	15-19
Power Supply A, B	15-19
Board	15-20
1.9/2.5V Status, 3.3V Status, 5V Status	15-20
Monitor System Status SEP	15-20
SEP redundancy	15-20
Refresh	15-21
Back	15-21
SEP	15-21
Status	15-22
DSP Code Version	15-22
Inbound Hash: Octets / Packets	15-22
Outbound Hash: Octets / Packets	15-22
Encrypted: Octets / Packets	15-22
Decrypted: Octets / Packets	15-22
Hash Encrypted: Packets	15-22
Hash Decrypted: Packets	15-23
Drops: Packets	15-23
Random Requests	15-23
Random Replenishments	15-23
Random Bytes Available	15-23
Random Cache Empty	15-23
DH Keys Generated	15-23
DH Derived Secret Keys	15-23
RSA Digital Signings	15-24
RSA Digital Verifications	15-24
RSA Encryptions: Octets / Packets	15-24
RSA Decryptions: Octets / Packets	15-24
DSA Digital Keys Generated	15-24
DSA Digital Signings	15-24
DSA Digital Verifications	15-24
Monitor System Status LED Status	15-25
Refresh	15-25
[LED selector button]	15-25

Monitor Sessions	15-26
Refresh	15-26
Session Summary table	15-26
Active LAN-to-LAN Sessions	15-27
Active Remote Access Sessions	15-27
Active Management Sessions	15-27
Total Active Sessions	15-27
Peak Concurrent Sessions	15-27
Concurrent Sessions Limit	15-27
Total Cumulative Sessions	15-27
LAN-to-LAN Sessions table	15-27
[Remote Access Sessions Management Sessions]	15-27
Connection Name	15-27
IP Address	15-28
Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx	15-28
Remote Access Sessions table	15-28
[LAN-to-LAN Sessions Management Sessions]	15-28
Username	15-28
Public IP Address	15-28
Assigned IP Address	15-28
Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx	15-28
Management Sessions table	15-29
[LAN-to-LAN Sessions Remote Access Sessions]	15-29
Administrator	15-29
IP Address	15-29
Protocol, Encryption, Login Time, Duration	15-29
Monitor Sessions Detail	15-30
Refresh	15-34
Back to Sessions	15-34
Monitor Sessions Detail parameters	15-34
Monitor Sessions Protocols	15-36
Refresh	15-36
Active Sessions	15-36
Total Sessions	15-36
Protocol	15-36
Sessions	15-37
Bar Graph	15-37
Percentage	15-37
Monitor Sessions SEPs	15-38
Refresh	15-38
Active Sessions	15-38
Total Sessions	15-38
SEP	15-38
Sessions	15-38
Bar Graph	15-39
Percentage	15-39
Monitor Sessions Encryption	15-39
Refresh	15-39
Active Sessions	15-39
Total Sessions	15-39
Encryption	15-40
Sessions	15-40

Bar Graph	15-40
Percentage	15-40
Monitor Sessions Top Ten Lists	15-41
Monitor Sessions Top Ten Lists Data	15-41
Refresh	15-41
Username	15-41
IP Address	15-42
Protocol	15-42
Encryption	15-42
Login Time	15-43
Total Bytes	15-43
Monitor Sessions Top Ten Lists Duration	15-43
Refresh	15-43
Username	15-43
IP Address	15-43
Protocol	15-44
Encryption	15-44
Login Time	15-44
Duration	15-45
Monitor Sessions Top Ten Lists Throughput	15-45
Refresh	15-45
Username	15-45
IP Address	15-45
Protocol	15-45
Encryption	15-46
Login Time	15-46
Avg. Throughput (bytes/sec)	15-46
Monitor Statistics	15-47
Monitor Statistics PPTP	15-48
Refresh	15-48
Total Tunnels	15-48
Active Tunnels	15-48
Maximum Tunnels	15-48
Total Sessions	15-49
Active Sessions	15-49
Maximum Sessions	15-49
Rx Octets Control / Data	15-49
Rx Packets Control / Data	15-49
Rx Discards Control / Data	15-49
Tx Octets Control / Data	15-49
Tx Packets Control / Data	15-49
PPTP Sessions	15-49
Peer IP	15-50
Username	15-50
Receive Octets	15-50
Receive Packets	15-50
Receive Discards	15-50
Receive ZLB	15-50
Transmit Octets	15-50
Transmit Packets	15-50
Transmit ZLB	15-50
ACK Timeouts	15-50
Flow	15-51

Monitor Statistics L2TP	15-51
Refresh	15-51
Total Tunnels	15-52
Active Tunnels	15-52
Maximum Tunnels	15-52
Failed Tunnels	15-52
Total Sessions	15-52
Active Sessions	15-52
Maximum Sessions	15-52
Failed Sessions	15-52
Rx Octets Control / Data	15-52
Rx Packets Control / Data	15-53
Rx Discards Control / Data	15-53
Tx Octets Control / Data	15-53
Tx Packets Control / Data	15-53
L2TP Sessions	15-53
Remote IP	15-53
Username	15-53
Serial	15-53
Receive Octets	15-53
Receive Packets	15-54
Receive Discards	15-54
Receive ZLB	15-54
Transmit Octets	15-54
Transmit Packets	15-54
Transmit ZLB	15-54
Monitor Statistics IPSec	15-55
Refresh	15-55
IKE (Phase 1) Statistics	15-56
Active Tunnels	15-56
Total Tunnels	15-56
Received Bytes	15-56
Sent Bytes	15-56
Received Packets	15-56
Sent Packets	15-56
Received Packets Dropped	15-56
Sent Packets Dropped	15-56
Received Notifies	15-57
Sent Notifies	15-57
Received Phase-2 Exchanges	15-57
Sent Phase-2 Exchanges	15-57
Invalid Phase-2 Exchanges Received	15-57
Invalid Phase-2 Exchanges Sent	15-57
Rejected Received Phase-2 Exchanges	15-57
Rejected Sent Phase-2 Exchanges	15-57
Phase-2 SA Delete Requests Received	15-57
Phase-2 SA Delete Requests Sent	15-58
Initiated Tunnels	15-58
Failed Initiated Tunnels	15-58
Failed Remote Tunnels	15-58
Authentication Failures	15-58
Decryption Failures	15-58
Hash Validation Failures	15-58

System Capability Failures	15-58
No-SA Failures	15-58
IPSec (Phase 2) Statistics	15-59
Active Tunnels	15-59
Total Tunnels	15-59
Received Bytes	15-59
Sent Bytes	15-59
Received Packets	15-59
Sent Packets	15-59
Received Packets Dropped	15-59
Received Packets Dropped (Anti-Replay)	15-59
Sent Packets Dropped	15-60
Inbound Authentications	15-60
Failed Inbound Authentications	15-60
Outbound Authentications	15-60
Failed Outbound Authentications	15-60
Decryptions	15-60
Failed Decryptions	15-60
Encryptions	15-60
Failed Encryptions	15-60
System Capability Failures	15-61
No-SA Failures	15-61
Protocol Use Failures	15-61
Monitor Statistics HTTP	15-61
Refresh	15-61
Octets Sent	15-61
Octets Received	15-61
Packets Sent	15-62
Packets Received	15-62
Active Connections	15-62
Max Connections	15-62
Monitor Statistics Events	15-62
Refresh	15-63
Event Class	15-63
Event Number	15-63
Count of Events	15-63
Monitor Statistics Telnet	15-63
Refresh	15-63
Active Sessions	15-64
Attempted Sessions	15-64
Successful Sessions	15-64
Telnet Sessions	15-64
Client IP Address:Port	15-64
Inbound Octets Total	15-64
Inbound Octets Command	15-64
Inbound Octets Discarded	15-64
Outbound Octets Total	15-64
Outbound Octets Dropped	15-64
Monitor Statistics DNS	15-65
Refresh	15-65
Requests	15-65
Responses	15-65

Timeouts	15-65
Server Unreachable	15-65
Other Failures	15-65
Monitor Statistics Authentication	15-66
Refresh	15-66
Server IP Address:Port	15-66
Requests	15-66
Retransmissions	15-66
Accepts	15-66
Rejects	15-67
Challenges	15-67
Malformed Responses	15-67
Bad Authenticators	15-67
Pending Requests	15-67
Timeouts	15-67
Unknown Type	15-67
Monitor Statistics Accounting	15-68
Refresh	15-68
Server IP Address:Port	15-68
Requests	15-68
Retransmissions	15-68
Responses	15-68
Malformed Responses	15-68
Bad Authenticators	15-69
Pending Requests	15-69
Timeouts	15-69
Unknown Type	15-69
Monitor Statistics Filtering	15-69
Refresh	15-69
Interface	15-70
Inbound Packets Pre-Filter	15-70
Inbound Packets Filtered	15-70
Inbound Packets Post Filter	15-70
Outbound Packets Pre-Filter	15-70
Outbound Packets Filtered	15-70
Outbound Packets Post Filter	15-70
Monitor Statistics VRRP	15-71
Refresh	15-71
Checksum Errors	15-71
Version Errors	15-71
VRID Errors	15-72
VRID	15-72
Virtual Routers	15-72
Interface: 1 (Private), 2 (Public), 3 (External)	15-72
Status	15-72
Became Master	15-72
Advertisements Received	15-72
Advertisement Interval Errors	15-72
Authentication Failures	15-72
Time-to-Live Errors	15-73
Priority 0 Packets Received	15-73
Priority 0 Packets Sent	15-73

Invalid Type Received	15-73
Address List Errors	15-73
Invalid Authentication Errors	15-73
Mismatch Authentication Errors	15-73
Packet Length Errors	15-73
Monitor Statistics SSL	15-74
Refresh	15-74
Unencrypted Inbound Octets	15-74
Encrypted Inbound Octets	15-74
Unencrypted Outbound Octets	15-74
Encrypted Outbound Octets	15-74
Total Sessions	15-74
Active Sessions	15-75
Max Active Sessions	15-75
Monitor Statistics DHCP	15-75
Refresh	15-75
Leased IP Address	15-75
Lease Duration	15-75
Time Used	15-75
Time Left	15-76
DHCP Server Address	15-76
Monitor Statistics Address Pools	15-76
Refresh	15-76
IP Address Range: Start / End	15-76
Total Addresses	15-76
Available Addresses	15-76
Allocated Addresses	15-76
Max Allocated Addresses	15-77
Monitor Statistics MIB-II	15-77
Monitor Statistics MIB-II Interfaces	15-78
Refresh	15-78
Interface	15-78
Status	15-78
Unicast In	15-79
Unicast Out	15-79
Multicast In	15-79
Multicast Out	15-79
Broadcast In	15-79
Broadcast Out	15-79
Monitor Statistics MIB-II TCP/UDP	15-80
Refresh	15-80
TCP Segments Received	15-80
TCP Segments Transmitted	15-80
TCP Segments Retransmitted	15-80
TCP Timeout Min	15-80
TCP Timeout Max	15-81
TCP Connection Limit	15-81
TCP Active Opens	15-81
TCP Passive Opens	15-81
TCP Attempt Failures	15-81
TCP Established Resets	15-81
TCP Current Established	15-81

UDP Datagrams Received	15-81
UDP Datagrams Transmitted	15-81
UDP Errored Datagrams	15-82
UDP No Port	15-82
Monitor Statistics MIB-II IP	15-82
Refresh	15-82
Packets Received (Total)	15-82
Packets Received (Header Errors)	15-83
Packets Received (Address Errors)	15-83
Packets Received (Unknown Protocols)	15-83
Packets Received (Discarded)	15-83
Packets Received (Delivered)	15-83
Packets Forwarded	15-83
Outbound Packets Discarded	15-83
Outbound Packets with No Route	15-83
Packets Transmitted (Requests)	15-84
Fragments Needing Reassembly	15-84
Reassembly Successes	15-84
Reassembly Failures	15-84
Fragmentation Successes	15-84
Fragmentation Failures	15-84
Fragments Created	15-84
Monitor Statistics MIB-II RIP	15-85
Refresh	15-85
Global Route Changes	15-85
Global Queries	15-85
Interfaces	15-85
Interface Address	15-85
Received Bad Packets	15-85
Received Bad Routes	15-86
Sent Updates	15-86
Monitor Statistics MIB-II OSPF	15-87
Refresh	15-87
Router ID	15-88
Version	15-88
External LSA Count	15-88
External LSA Checksum	15-88
LSAs Originated	15-88
New LSAs Received	15-88
LSA Database Limit	15-88
Designated Routers	15-88
Interface Address	15-89
Interface Name	15-89
Designated Router	15-89
Backup Designated Router	15-89
Neighbors	15-89
IP Address	15-89
Router ID	15-89
State	15-90
Areas	15-90
Area ID	15-90
SPF Runs	15-90
AS Border Routers	15-90

Area Border Routers	15-90
Area LSA Count	15-91
Area LSA Checksum	15-91
External LSAs	15-91
Area ID	15-91
Type	15-91
Link State ID	15-91
Router ID	15-91
Sequence	15-91
Age	15-91
Monitor Statistics MIB-II ICMP	15-92
Refresh	15-92
Total Received / Transmitted	15-92
Errors Received / Transmitted	15-92
Destination Unreachable Received / Transmitted	15-92
Time Exceeded Received / Transmitted	15-93
Parameter Problems Received / Transmitted	15-93
Source Quench Received / Transmitted	15-93
Redirects Received / Transmitted	15-93
Echo Requests (PINGs) Received / Transmitted	15-93
Echo Replies (PINGs) Received / Transmitted	15-93
Timestamp Requests Received / Transmitted	15-93
Timestamp Replies Received / Transmitted	15-93
Address Mask Requests Received / Transmitted	15-94
Address Mask Replies Received / Transmitted	15-94
Monitor Statistics MIB-II ARP Table	15-94
Refresh	15-94
Interface	15-95
Physical Address	15-95
IP Address	15-95
Mapping Type	15-95
Action / Delete	15-95
Monitor Statistics MIB-II Ethernet	15-96
Refresh	15-96
Interface	15-96
Alignment Errors	15-96
FCS Errors	15-96
Carrier Sense Errors	15-96
SQE Test Errors	15-97
Frame Too Long Errors	15-97
Deferred Transmits	15-97
Single Collisions	15-97
Multiple Collisions	15-97
Late Collisions	15-97
Excessive Collisions	15-97
MAC Errors: Transmit	15-97
MAC Errors: Receive	15-97
Speed (Mbps)	15-98
Duplex	15-98

Monitor Statistics MIB-II SNMP	15-98
Refresh	15-98
Requests Received	15-98
Bad Version	15-98
Bad Community String	15-99
Parsing Errors	15-99
Silent Drops	15-99
Proxy Drops	15-99

16 Using the Command Line Interface

Accessing the CLI	16-1
Console access	16-1
Telnet or Telnet/SSL access	16-2
Starting the CLI	16-2
Using the CLI	16-3
Choosing menu items	16-3
Entering values	16-3
Specifying configured items	16-4
Navigating quickly through the CLI	16-5
Using shortcut numbers	16-5
Using Back and Home	16-6
Getting Help Information	16-6
Saving the configuration file	16-7
Stopping the CLI	16-7
Understanding CLI access rights	16-7
CLI menu reference	16-8
Main menu	16-8
1 Configuration	16-8
1.1 Configuration > Interface Configuration	16-9
1.1.1, 1.1.2, or 1.1.3 Configuration > Interface Configuration > Configure Ethernet #1 or #2 or #3	16-9
1.1.4 Configuration > Interface Configuration > Configure Power Supplies	16-9
1.1.3 Configuration > Interface Configuration > Configure Power Supplies	16-10
1.1.5 Configuration > Interface Configuration > Configure Expansion Cards	16-10
1.1.4 Configuration > Interface Configuration > Configure Expansion Cards	16-10
1.2 Configuration > System Management	16-10
1.2.1 Configuration > System Management > Servers	16-11
1.2.2 Configuration > System Management > Address Management	16-11
1.2.3 Configuration > System Management > Tunneling Protocols	16-11
1.2.4 Configuration > System Management > IP Routing	16-11
1.2.5 Configuration > System Management > Management Protocols	16-12
1.2.6 Configuration > System Management > Event Configuration	16-12
1.2.7 Configuration > System Management > General Config	16-12
1.3 Configuration > User Management	16-12
1.3.1 Configuration > User Management > Base Group	16-13
1.3.2 Configuration > User Management > Groups	16-13
1.3.3 Configuration > User Management > Users	16-13
1.4 Configuration > Policy Management	16-13
1.4.1 Configuration > Policy Management > Access Hours	16-14
1.4.2 Configuration > Policy Management > Traffic Management	16-14
2 Administration	16-14
2.1 Administration > Administer Sessions	16-14
2.3 Administration > System Reboot	16-15

2.3.2 Administration > System Reboot > Schedule Reboot	16-15
2.3.3 Administration > System Reboot > Schedule Shutdown	16-15
2.5 Administration > Access Rights	16-15
2.5.1 Administration > Access Rights > Administrators	16-15
2.5.2 Administration > Access Rights > Access Control List	16-16
2.5.3 Administration > Access Rights > Access Settings	16-16
2.6 Administration > File Management	16-16
2.6.6 Administration > File Management > Swap Configuration File	16-16
2.7 Administration > Certificate Management	16-17
2.7.2 Administration > Certificate Management > Installation	16-17
2.7.3 Administration > Certificate Management > Certificate Authorities	16-17
2.7.4 Administration > Certificate Management > Identity Certificates	16-17
2.7.5 Administration > Certificate Management > SSL Certificate	16-18
3 Monitoring	16-18
3.1 Monitoring > Routing Table	16-18
3.2 Monitoring > Event Log	16-19
3.2.2 Monitoring > Event Log > View Event Log	16-19
3.3 Monitoring > System Status	16-19
3.3.2 Monitoring > System Status > View Card Status	16-19
3.4 Monitoring > Sessions	16-20
3.4.1 Monitoring > Sessions > View Session Statistics	16-20
3.4.2 Monitoring > Sessions > View Top Ten Lists	16-20
3.4.3 Monitoring > Sessions > View Session Protocols	16-20
3.4.4 Monitoring > Sessions > View Session SEPs	16-21
3.4.5* Monitoring > Sessions > View Session Encryption	16-21
3.5 Monitoring > General Statistics	16-21
3.5.1 Monitoring > General Statistics > Protocol Statistics	16-21
3.5.2 Monitoring > General Statistics > Server Statistics	16-22
3.5.3 Monitoring > General Statistics > Event Statistics	16-22
3.5.4 Monitoring > General Statistics > MIB II Statistics	16-22

A Errors and troubleshooting

Files for troubleshooting	A-1
Event logs	A-1
Crash dump file	A-1
Configuration files	A-2
VPN Concentrator Manager errors	A-2
Browser Refresh / Reload button logs out the Manager	A-2
Browser Back or Forward button displays an incorrect screen or incorrect data	A-2
Invalid Login or Session Timeout	A-3
Error / An error has occurred while attempting to perform...	A-4
You are using an old browser or have disabled JavaScript	A-5
Not Allowed / You do not have sufficient authorization...	A-6
Not Found / An error has occurred while attempting to access...	A-7
Microsoft Internet Explorer Script Error: No such interface supported	A-7
Command Line Interface errors	A-8
ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID.	A-8
ERROR:-- Out of Range value entered. Try again.	A-8
ERROR:-- The Passwords do not match. Please try again.	A-8

LED indicators	A-9
VPN Concentrator LEDs (front)	A-10
VPN Concentrator LEDs (rear)	A-11
SEP (Scalable Encryption Processing) Module LEDs (Model 3015–3080 only)	A-11
WAN Interface Module LEDs	A-12

B Copyrights, licenses, and notices

Software License Agreement of Cisco Systems, Inc.	B-1
Other licenses	B-3
Regulatory Agency Notices	B-9
Notice to Users of T1 Service	B-9
Notice to Users of Certified Component Devices	B-10
Affidavit (Appendix A)	B-11

Index

Tables

Table 5-1: RADIUS accounting record attributes	5-12
Table 7-1: Cisco-supplied default IKE Proposals	7-20
Table 10-1: VPN Concentrator event classes	10-1
Table 10-2: VPN Concentrator event severity levels	10-4
Table 10-3: Configuring “well-known” SNMP traps	10-8
Table 13-1: Cisco-supplied default filter rules	13-10
Table 13-2: Cisco-supplied default Security Associations	13-21
Table 13-3: Cisco-supplied default filters	13-30
Table 14-1: Parameter definitions for Administration Sessions screen	14-7
Table 14-2: Parameter definitions for Administration Sessions Detail screens	14-12
Table 14-3: Cisco-supplied default administrator rights	14-24
Table 15-1: Parameter definitions for Monitor Sessions screen	15-29
Table 15-2: Parameter definitions for Monitor Sessions Detail screens	15-34



Preface

About this manual

The *VPN 3000 Concentrator Series User Guide* provides guidelines for configuring the Cisco VPN 3000 Concentrator, details on all the functions available in the VPN 3000 Concentrator Series Manager, and instructions for using the VPN 3000 Concentrator Series Command Line Interface.

Prerequisites

We assume you have read the *VPN 3000 Concentrator Series Getting Started* manual and have followed the minimal configuration steps in Quick Configuration. That section of the VPN Concentrator Manager is not described here.

We also assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices may be new to you. You should be familiar with Windows® 95/98 or Windows NT® system configuration and management, and you should be familiar with Microsoft Internet Explorer or Netscape® Navigator® or Communicator browsers.

Organization

This manual is organized by the order in which sections appear in the VPN Concentrator Manager table of contents (the left frame of the Manager browser window; see Figure 1-30 in Chapter 1).

Chapter 1, *Using the VPN 3000 Concentrator Series Manager* explains how to log in, navigate, and use the VPN Concentrator Manager with a browser. It explains both HTTP and HTTPS browser connections, and how to install the SSL certificate for a secure (HTTPS) connection.

Chapter 2, *Configuration* describes the main VPN Concentrator Manager configuration screen.

Chapter 3, *Interfaces* explains how to configure the VPN Concentrator Ethernet and WAN interfaces, and how to configure the system power supply and voltage sensor alarms.

Chapter 4, *System Configuration* describes the system configuration screen of the VPN Concentrator Manager.

Chapter 5, *Servers* explains how to configure the VPN Concentrator to communicate with and access servers for user authentication, user accounting, converting hostnames to IP addresses (DNS), assigning client IP addresses (DHCP), and network time synchronization (NTP).

Chapter 6, *Address Management* explains how to configure client IP addresses available in your private network addressing scheme, that let the client function as a VPN tunnel endpoint.

Chapter 7, *Tunneling Protocols* explains how to configure system-wide parameters for PPTP and L2TP, how to configure IPSec LAN-to-LAN connections, and how to configure IKE proposals for IPSec. These are the three most popular VPN tunneling protocols.

Chapter 8, *IP Routing* explains how to configure static routes, default gateways, and OSPF in the VPN Concentrator IP routing subsystem; how to configure DHCP global parameters; and how to configure redundant systems using VRRP.

Chapter 9, *Management Protocols* explains how to configure built-in VPN Concentrator servers that provide management functions: FTP, HTTP and HTTPS, TFTP, Telnet, SNMP, and SSL.

Chapter 10, *Events* explains how to configure system events such as alarms, traps, error conditions, network problems, task completion, or status changes. You can specify several ways to record and send event messages.

Chapter 11, *General* explains how to configure the system identification, date, and time.

Chapter 12, *User Management* explains how to configure groups and users with attributes that determine their access to and use of the VPN. Configuring groups and users correctly is essential for managing the security of your VPN.

Chapter 13, *Policy Management* explains how to configure network lists, filters, rules, and Security Associations, which are policies that govern what data traffic can flow through the VPN. You should develop and configure policies first, since you apply them to groups, users, and interfaces. This chapter also describes NAT configuration.

Chapter 14, *Administration* explains how to configure and use high-level VPN Concentrator administrator activities such as who is allowed to configure the system, what software runs on it, rebooting and shutting down the system, managing its files, and managing X.509 digital certificates.

Chapter 15, *Monitoring* explains the many status, statistics, sessions, and event log screens that you can use to monitor the VPN Concentrator.

Chapter 16, *Using the Command Line Interface* explains how to use the built-in menu- and command-line-based administrative management system via the system console or a Telnet session. With the CLI, you can access and configure all the same parameters as the HTML-based VPN Concentrator Manager.

Appendix A, *Errors and troubleshooting* describes common errors that may occur while configuring the system, and how to correct them. It also describes all system and module LED indicators.

Appendix B, *Copyrights, licenses, and notices* provides all copyright and license information for Cisco software on the VPN Concentrator, and for software that the system uses under license from other firms.

Additional Documentation

The *VPN 3000 Concentrator Series Getting Started* manual provides information to take you from unpacking and installing the VPN Concentrator, through configuring the minimal parameters to make it operational (called Quick Configuration).

The VPN Concentrator Manager also includes extensive context-sensitive online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

The *VPN 3000 Client User Guide* explains how to install, configure, and use the Cisco VPN 3000 Client, which lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN Concentrator.

The *VPN 3000 Monitor User Guide* explains how to install, set up, and use the VPN 3000 Monitor, which is a separate Java™ application that polls VPN 3000 Concentrators in a network for information and displays that information on your workstation.

The *VPN 3000 Concentrator Series Getting Started* manual, this *VPN 3000 Concentrator Series User Guide*, and the *VPN 3000 Client User Guide* are provided on the system software distribution CD-ROM in PDF format. To view the latest versions on the Cisco Technical Documentation Web site, click the **Support** tab on the toolbar at the top of the VPN Concentrator Manager window, and click the **Documentation** link.

Other references

Other useful books and articles include:

Frequently Asked Questions about Microsoft VPN Security. Microsoft Corporation: 1998. (Available from Microsoft web site, www.microsoft.com.)

Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.

Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.

Stallings, William. *Data and Computer Communications*, 5th ed. Prentice-Hall: 1997.

Understanding Point-to-Point Tunneling Protocol (PPTP). Microsoft Corporation: 1997. (Available from Microsoft web site.)

Virtual Private Networking: An Overview. Microsoft Corporation: 1999. (Available from Microsoft web site.)

www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

www.whatis.com, a Web reference site with definitions for computer, networking, and data communication terms.

Documentation Conventions

We use these typographic conventions in this manual:

Font	Meaning
This font	Document, chapter, and section titles. Emphasized text.
This font	Command-line prompts and entries, data-entry-field entries, system displays, filenames, etc.
<u>This font</u>	Literal entries you should make exactly as shown.
<This font>	Variables that the system supplies. Ignore the angle brackets.
This font	Menus, menu items, keyboard keys, icons, screen names, data-entry field names, etc.

Data Formats

As you configure and manage the system, enter data in these formats unless the instructions indicate otherwise.

IP addresses

IP addresses use 4-byte dotted decimal notation; for example, 192 . 168 . 12 . 34. You can omit leading zeros in a byte position.

Subnet masks and wildcard masks

Subnet masks use 4-byte dotted decimal notation; for example, 255 . 255 . 255 . 0. Wildcard masks are the reverse of subnet masks and use the same notation; for example, 0 . 0 . 0 . 255. You can omit leading zeros in a byte position.

MAC addresses

MAC addresses use 6-byte hexadecimal notation; for example, 00 . 10 . 5A . 1F . 4F . 07.

Hostnames

Hostnames use legitimate network host or end-system name notation; for example, VPN01. Spaces are not allowed. A hostname must uniquely identify a specific system on a network.

Text strings

Text strings use alphanumeric characters, upper- and lower-case. Most text strings are case-sensitive; for example, *simon* and *Simon* represent different usernames. The maximum length of text strings is generally 48 characters.

Filenames

Filenames on the VPN Concentrator follow the DOS 8.3 naming convention: a maximum of eight characters for the name, plus a maximum of three characters for an extension. For example, LOG00007 . TXT is a legitimate filename. The VPN Concentrator always stores filenames as uppercase.

Port numbers

Port numbers use decimal numbers from 0 to 65535 with no commas or spaces.

Contacting Cisco with questions

Cisco provides extensive technical support through its own staff and through authorized agents. If you have questions, we suggest you first try the Cisco Web site at www.cisco.com, and go to the **Service & Support** section. From there you can go to additional support areas such as the Technical Assistance Center (TAC), software updates, technical documentation, and service and support solutions.

To phone the North America Technical Assistance Center, call **800 553-2447** or **+1 408 526-7209**.

End of Preface



Using the VPN 3000 Concentrator Series Manager

The VPN 3000 Concentrator Series Manager is an HTML-based interface that lets you configure, administer, monitor, and manage the VPN 3000 Concentrator with a standard Web browser. To use it, you need only to connect to the VPN Concentrator using a PC and browser on the same private network with the VPN Concentrator.

The Manager uses the standard Web client / server protocol, HTTP (Hypertext Transfer Protocol), which is a cleartext protocol. However, you can also use the Manager in a secure, encrypted HTTP connection over SSL (Secure Sockets Layer) protocol, which is known as HTTPS.

- To use a cleartext HTTP connection, see *Connecting to the VPN Concentrator using HTTP*.
- To use HTTP over SSL (HTTPS) with the Manager:
 - 1 The first time, connect to the Manager using HTTP, and
 - 2 Install an SSL certificate in the browser; see *Installing the SSL certificate in your browser* on page 1-3.

Once the SSL certificate is installed, you can connect directly using HTTPS; see *Connecting to the VPN Concentrator using HTTPS* on page 1-17.

Browser requirements

The VPN Concentrator Manager requires either Microsoft Internet Explorer version 4.0 or higher, or Netscape Navigator / Communicator version 4.0 or higher. For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

JavaScript

Be sure JavaScript is enabled in the browser. Check these settings:

- Internet Explorer 4.0:
 - On the **View** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom (for expert users)** then click **Settings**.
 - In the **Security Settings** window, scroll down to **Scripting**.
 - Click **Enable** under **Scripting of Java applets**.
 - Click **Enable** under **Active scripting**.

- Internet Explorer 5.0:
 - On the **Tools** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom Level**.
 - In the **Security Settings** window, scroll down to **Scripting**.
 - Click **Enable** under **Active scripting**.
 - Click **Enable** under **Scripting of Java applets**.
- Navigator / Communicator 4.5:
 - On the **Edit** menu, select **Preferences**.
 - On the **Advanced** screen, check the box for **Enable JavaScript**.

Cookies

Be sure cookies are enabled in the browser. Check these settings:

- Internet Explorer 4.0:
 - On the **View** menu, select **Internet Options**.
 - On the **Advanced** tab, scroll down to **Security** then **Cookies**.
 - Click **Always accept cookies**.
- Internet Explorer 5.0:
 - On the **Tools** menu, select **Internet Options**.
 - On the **Security** tab, click **Custom Level**.
 - In the **Security Settings** window, scroll down to **Cookies**.
 - Click **Enable** under **Allow cookies that are stored on your computer**.
 - Click **Enable** under **Allow per-session cookies (not stored)**.
- Navigator / Communicator 4.5:
 - On the **Edit** menu, select **Preferences**.
 - On the **Advanced** screen, click one of the **Accept ... cookies** choices, and *do not* check **Warn me before accepting a cookie**.

Navigation toolbar

Do not use the *browser* navigation toolbar buttons **Back**, **Forward**, or **Refresh / Reload** with the VPN Concentrator Manager unless instructed to do so. To protect access security, clicking **Refresh / Reload** automatically logs out the Manager session. Clicking **Back** or **Forward** may display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN Concentrator Manager.

Recommended PC monitor / display settings

For best ease of use, we recommend setting your monitor or display:

- Desktop area = 1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette = 256 colors or higher.

Connecting to the VPN Concentrator using HTTP

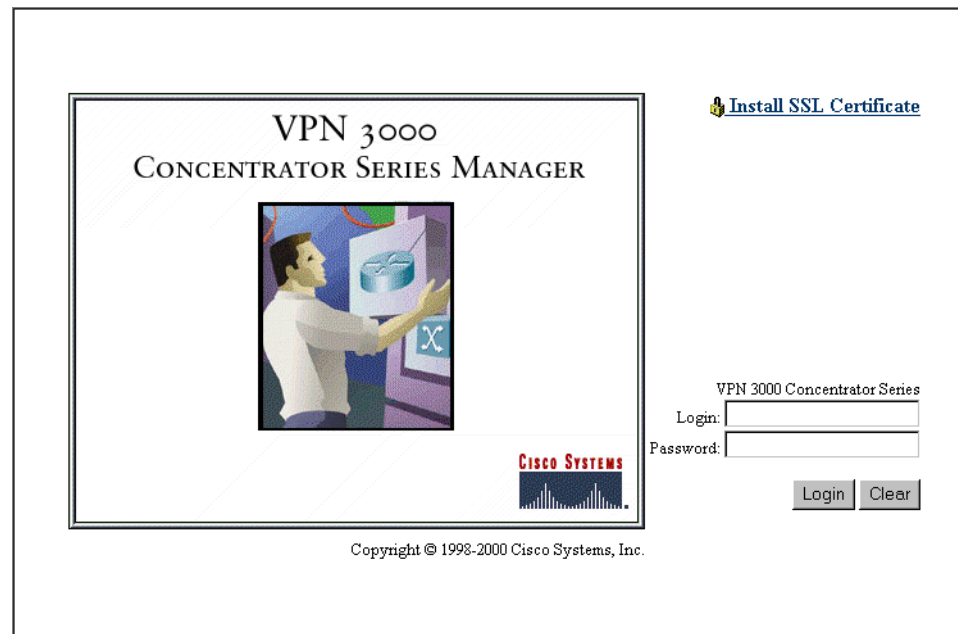
When your system administration tasks and network permit a cleartext connection between the VPN Concentrator and your browser, you can use the standard HTTP protocol to connect to the system.

Even if you plan to use HTTPS, you use HTTP at first to install an SSL certificate in your browser.

- 1 Bring up the browser.
- 2 In the browser **Address** or **Location** field, you can just enter the VPN Concentrator Ethernet 1 (Private) interface IP address; e.g., 10.10.147.2. The browser automatically assumes and supplies an `http://` prefix.

The browser displays the VPN Concentrator Manager login screen.

Figure 1-1: VPN Concentrator Manager login screen



To continue using HTTP for the whole session, skip to *Logging in the VPN Concentrator Manager* on page 1-18.

Installing the SSL certificate in your browser

The VPN Concentrator Manager provides the option of using HTTP over SSL with the browser. SSL creates a secure session between your browser (client) and the VPN Concentrator (server). This protocol is known as HTTPS, and uses the `https://` prefix to connect to the server. The browser first authenticates the server, then they encrypt all data passed during the session.

HTTPS is often confused with a similar protocol, S-HTTP (Secure HTTP), which encrypts only HTTP application-level data. SSL encrypts *all* data between client and server at the IP socket level, and is thus more secure.

SSL uses digital certificates for authentication. The VPN Concentrator creates a self-signed SSL server certificate when it boots, and this certificate must be installed in the browser. Once the certificate is

installed, you can connect using HTTPS. You need to install the certificate from a given VPN Concentrator only once.

Managing the VPN Concentrator is the same with or without SSL. Manager screens may take slightly longer to load with SSL because of encryption / decryption processing. When connected via SSL, the browser shows a locked-padlock icon on its status bar. Both Microsoft Internet Explorer and Netscape Navigator support SSL.

Follow these steps to install and use the SSL certificate for the first time. We provide separate instructions for Internet Explorer and Netscape Navigator when they diverge.

- 1 Connect to the VPN Concentrator using HTTP as above.
- 2 On the login screen, click the **Install SSL Certificate** link.

The Manager displays the **Install SSL Certificate** screen and automatically begins to download and install its SSL certificate in your browser.

Figure 1-2: Install SSL Certificate screen

Install the SSL Certificate

Step 1: Download the SSL Certificate

The VPN 3000 Concentrator Series supports HTTP over SSL, also known as HTTPS. This requires the use of SSL digital certificates. A digital certificate has already been created for this VPN 3000 Concentrator Series. It will automatically download to your browser. **You should wait a few seconds for the certificate to be downloaded.**

**In a few seconds, a *File Download* dialog will appear for the SSL certificate.
Select *Open this file from its current location* to automatically install the SSL certificate.**

(If you chose **Save this file to disk**, double-clicking the file will install the certificate into Internet Explorer.)

The certificate only needs to be installed once per VPN 3000 Concentrator Series. If you installed a new SSL certificate onto the VPN 3000 Concentrator Series, you may already have this certificate in your browser. *If the certificate does not automatically download after one minute, [click here to install it](#).*

Step 2: Connect to the VPN 3000 Concentrator Series using SSL

To use SSL, use the protocol identifier **https:** rather than **http:** when accessing the VPN 3000 Concentrator Series (e.g. <https://10.10.147.2>). [After installing the SSL certificate, click here to connect to the VPN 3000 Concentrator Series using SSL.](#)

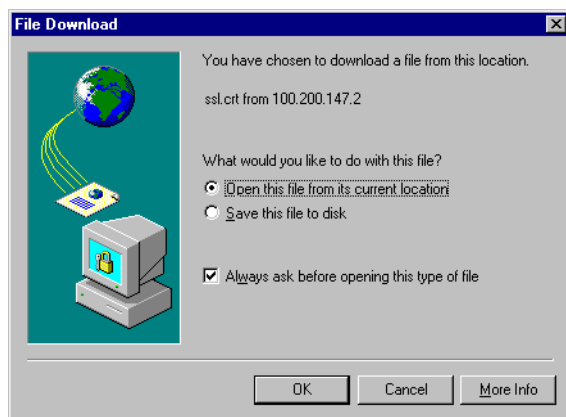
The installation sequence now differs depending on the browser. Continue below for Internet Explorer, or skip to *Installing the SSL certificate with Netscape* on page 1-10.

Installing the SSL certificate with Internet Explorer

This section describes SSL certificate installation using Microsoft Internet Explorer 5.0. (With Internet Explorer 4.0, some dialog boxes may differ but the process is similar.)

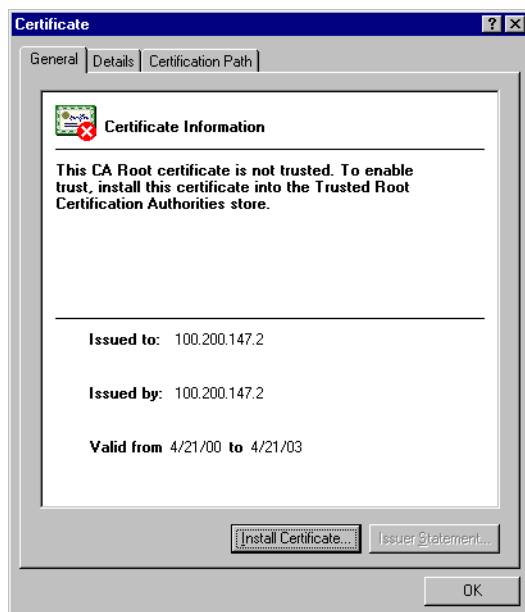
You need to install the SSL certificate from a given VPN Concentrator only once. If you do reinstall it, the browser repeats all these steps each time.

A few seconds after the VPN Concentrator Manager SSL screen appears, Internet Explorer displays a **File Download** dialog box that identifies the certificate filename and source, and asks whether to **Open** or **Save** the certificate. To immediately install the certificate in the browser, select **Open**. If you **Save** the file, the browser prompts for a location; you must then double-click on the file to install it.

Figure 1-3: Internet Explorer File Download dialog box

3 Click the **Open this file from its current location** radio button, then click **OK**.

The browser displays the **Certificate** dialog box with information about the certificate. You must now install the certificate.

Figure 1-4: Internet Explorer Certificate dialog box

4 Click **Install Certificate**.

The browser starts a wizard to install the certificate. The certificate store is where such certificates are stored in Internet Explorer.

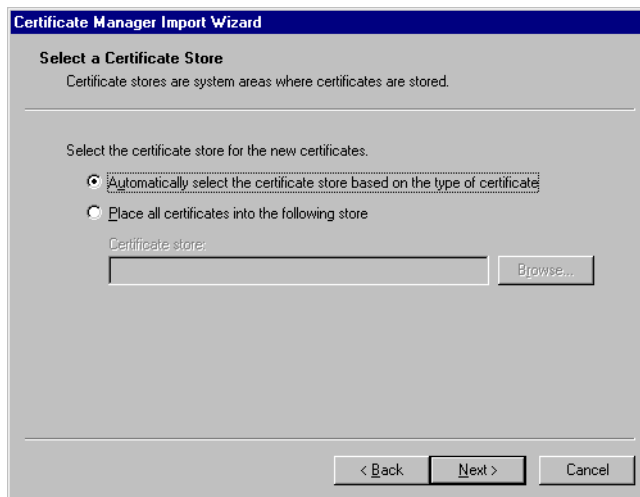
Figure 1-5: Internet Explorer Certificate Manager Import Wizard dialog box



5 Click **Next** to continue.

The wizard opens the next dialog box asking you to select a certificate store.

Figure 1-6: Internet Explorer Certificate Manager Import Wizard dialog box

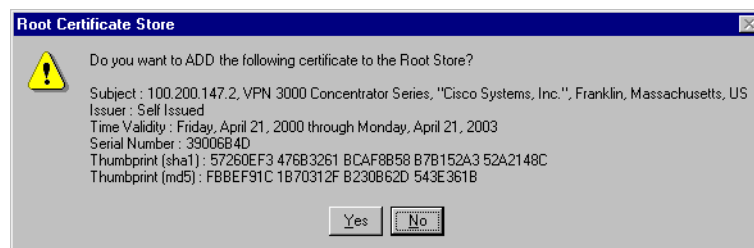
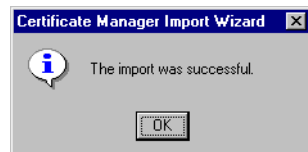


6 Let the wizard **Automatically select the certificate store**, and click **Next**.

The wizard opens a dialog box to complete the installation.

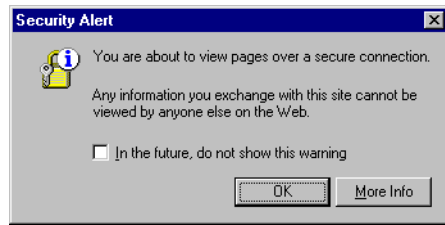
Figure 1-7: Internet Explorer Certificate Manager Import Wizard dialog box**7** Click **Finish**.

The wizard opens the **Root Certificate Store** dialog box asking you to confirm the installation.

Figure 1-8: Internet Explorer Root Certificate Store dialog box**8** To install the certificate, click **Yes**. This dialog box closes, and a final wizard confirmation dialog box opens.**Figure 1-9: Internet Explorer Certificate Manager Import Wizard final dialog box****9** Click **OK** to close this dialog box, and click **OK** on the **Certificate** dialog box (Figure 1-4) to close it. You can now connect to the VPN Concentrator using HTTP over SSL (HTTPS).**10** On the Manager SSL screen (Figure 1-2), click the link that says, **After installing the SSL certificate, click here to connect to the VPN 3000 Concentrator Series using SSL**.

Depending on how your browser is configured, you may see a **Security Alert** dialog box.

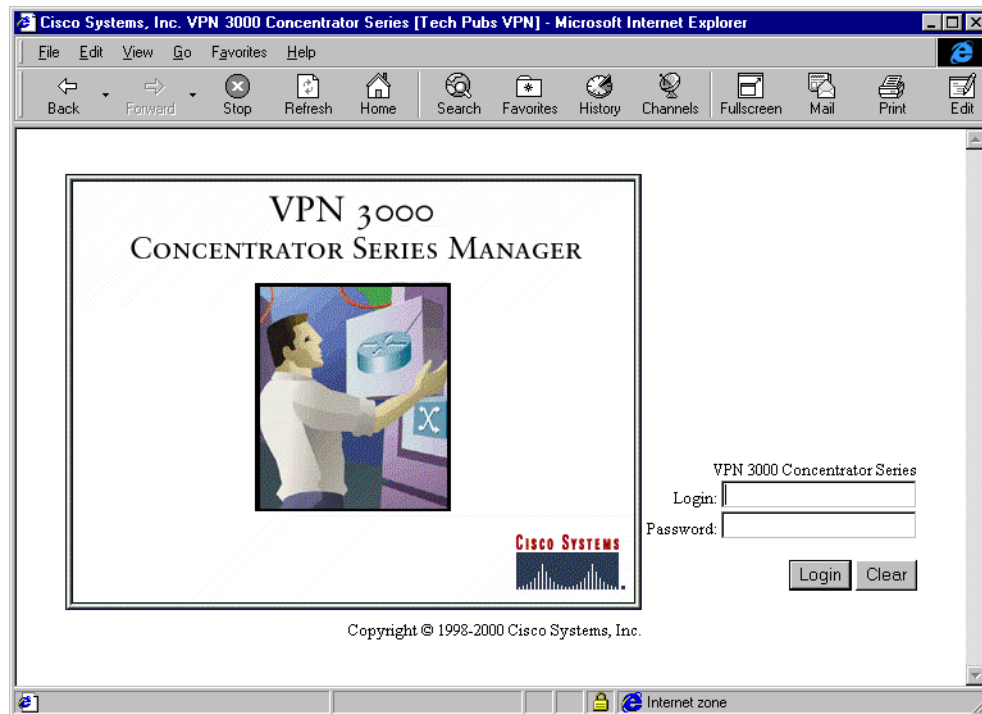
Figure 1-10: Internet Explorer Security Alert dialog box



11 Click **OK**.

The VPN Concentrator displays the HTTPS version of the Manager login screen.

Figure 1-11: VPN Concentrator Manager login screen using HTTPS (Internet Explorer)



The browser maintains the HTTPS state until you close it or access an unsecure site; in the latter case you may see a **Security Alert** screen.

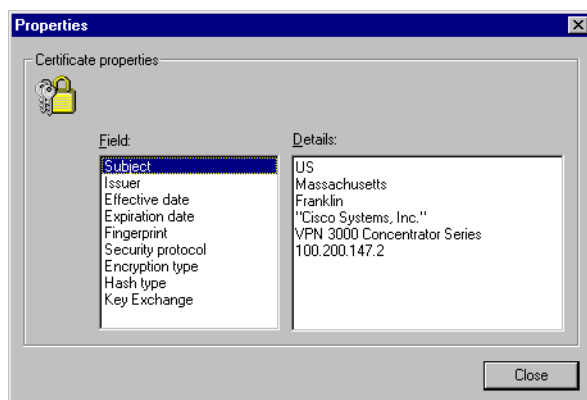
Proceed to *Logging in the VPN Concentrator Manager* on page 1-18 to log in as usual.

Viewing certificates with Internet Explorer

There are (at least) two ways to examine certificates stored in Internet Explorer.

First, note the padlock icon on the browser status bar in Figure 1-11. If you double-click on the icon, the browser opens a **Certificate Properties** screen showing details of the specific certificate in use.

Figure 1-12: Internet Explorer 4.0 Certificate Properties screen



Click any of the **Field** items to see **Details**. Click **Close** when finished.

Second, you can view all the certificates that are stored in Internet Explorer 4.0. Click the browser **View** menu and select **Internet Options**. Click the **Content** tab, then click **Authorities** in the **Certificates** section.

In Internet Explorer 5.0, click the browser **Tools** menu and select **Internet Options**. Click the **Content** tab, then click **Certificates** in the **Certificates** section. On the **Certificate Manager**, click the **Trusted Root Certification Authorities** tab.

The VPN Concentrator SSL certificate name is its Ethernet 1 (Private) IP address.

Figure 1-13: Internet Explorer 4.0 Certificate Authorities list



Select a certificate, then click **View Certificate**. The browser displays the **Certificate Properties** screen, as in Figure 1-12 above.

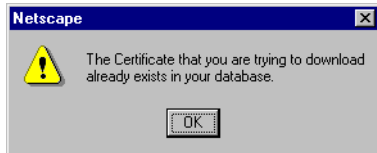
Installing the SSL certificate with Netscape

This section describes SSL certificate installation using Netscape Navigator / Communicator 4.5.

Reinstallation

You need to install the SSL certificate from a given VPN Concentrator only once. If you try to reinstall it, Netscape displays the note in Figure 1-14. Click **OK** and just connect to the VPN Concentrator using SSL (see Step 7 on page 1-13).

Figure 1-14: Netscape reinstallation note



First-time installation

The instructions below follow from Step 2 on page 1-4 and describe first-time certificate installation.

A few seconds after the VPN Concentrator Manager SSL screen appears, Netscape displays a **New Certificate Authority** screen.

Figure 1-15: Netscape New Certificate Authority screen 1



1 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which further explains the process.

Figure 1-16: Netscape New Certificate Authority screen 2

2 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which lets you examine details of the VPN Concentrator SSL certificate.

Figure 1-17: Netscape New Certificate Authority screen 3

3 Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, with choices for using the certificate. No choices are checked by default.

Figure 1-18: Netscape New Certificate Authority screen 4



- 4 You must check at least the first box, **Accept this Certificate Authority for Certifying network sites**. Click **Next>** to proceed.

Netscape displays the next **New Certificate Authority** screen, which lets you choose to have the browser warn you about sending data to the VPN Concentrator.

Figure 1-19: Netscape New Certificate Authority screen 5



- 5 Checking the box is optional. Doing so means that you get a warning whenever you apply settings on a Manager screen, so it's probably less intrusive to manage the VPN Concentrator without those warnings. Click **Next>** to proceed.

Netscape displays the final **New Certificate Authority** screen, which asks you to name the certificate.

Figure 1-20: Netscape New Certificate Authority screen 6

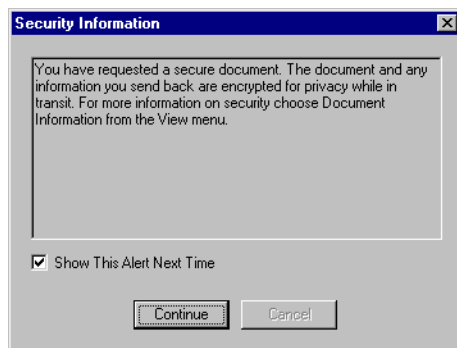
- 6** In the **Nickname** field, enter a descriptive name for this certificate. “Nickname” is something of a misnomer. We suggest you use a clearly descriptive name such as `Cisco VPN Concentrator 10.10.147.2`. This name appears in the list of installed certificates; see *Viewing certificates with Netscape* below.

Click **Finish**.

You can now connect to the VPN Concentrator using HTTP over SSL (HTTPS).

- 7** On the Manager SSL screen (Figure 1-2), click the link that says, **After installing the SSL certificate, click here to connect to the VPN Concentrator using SSL**.

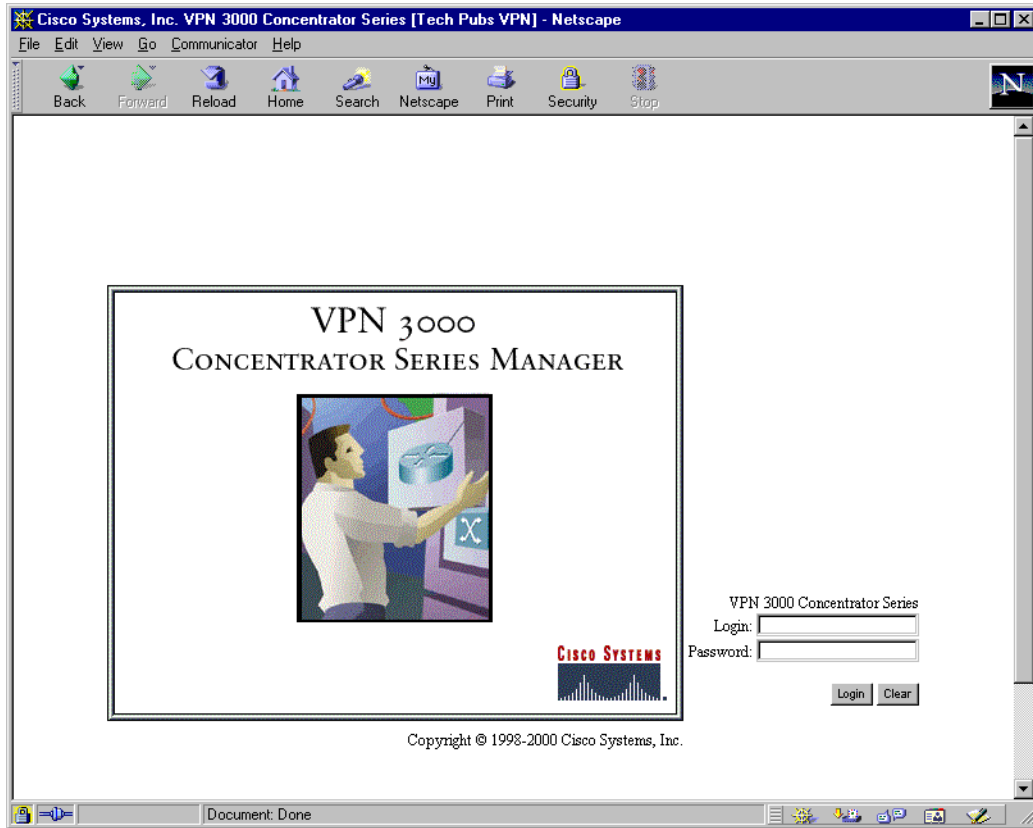
Depending on how your browser is configured, you may see a **Security Information Alert** dialog box.

Figure 1-21: Netscape Security Information Alert dialog box

- 8** Click **Continue**.

The VPN Concentrator displays the HTTPS version of the Manager login screen.

Figure 1-22: VPN Concentrator Manager login screen using HTTPS (Netscape)



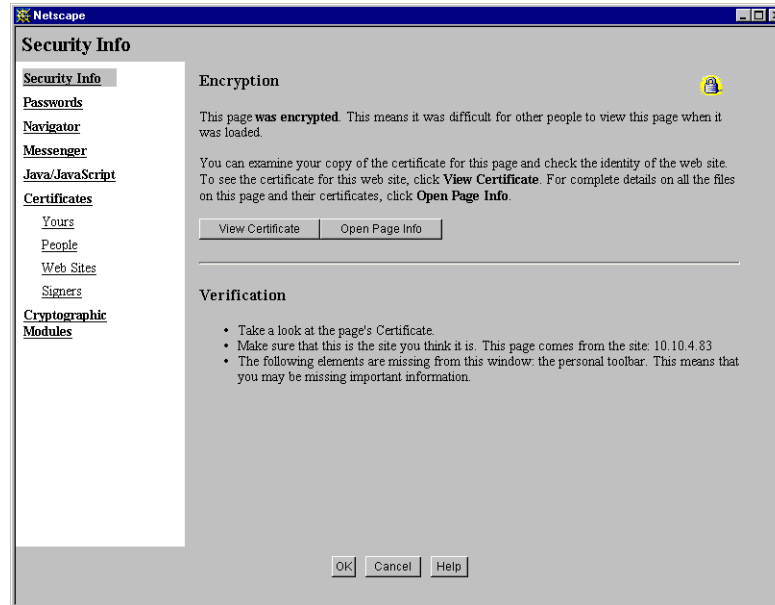
The browser maintains the HTTPS state until you close it or access an unsecure site; in the latter case, you may see a **Security Information Alert** dialog box.

Proceed to *Logging in the VPN Concentrator Manager* on page 1-18 to log in as usual.

Viewing certificates with Netscape

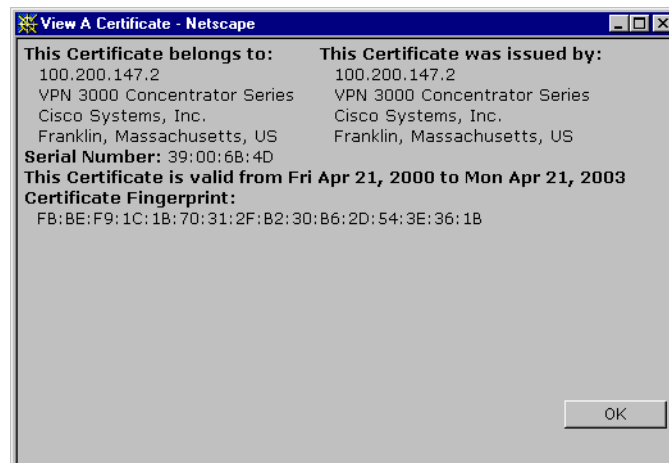
There are (at least) two ways to examine certificates stored in Netscape Navigator / Communicator 4.5. First, note the locked-padlock icon on the bottom status bar in Figure 1-22. If you click on the icon, Netscape opens a **Security Info** window. (You can also open this window by clicking **Security** on the Navigator Toolbar at the top of the Netscape window.)

Figure 1-23: Netscape Security Info window



Click **View Certificate** to see details of the specific certificate in use.

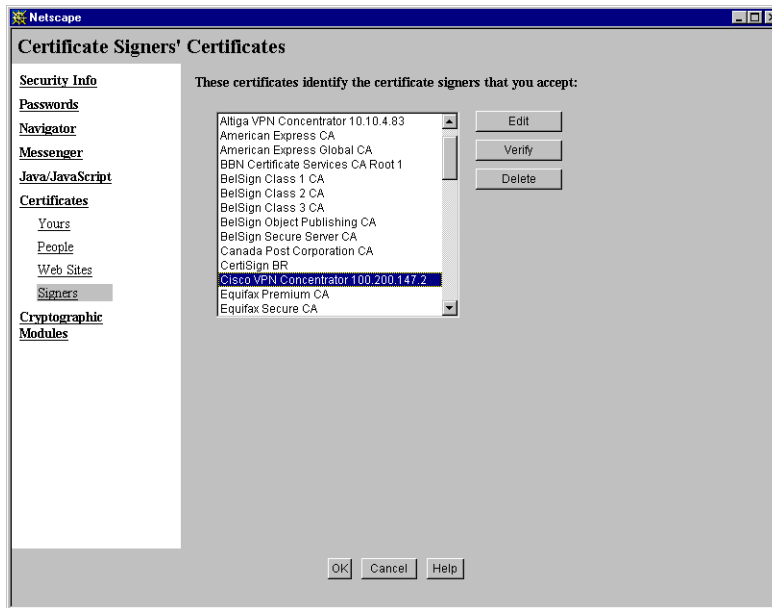
Figure 1-24: Netscape View Certificate screen



Click **OK** when finished.

Second, you can view all the certificates that are stored in Netscape. On the **Security Info** window, select **Certificates** then **Signers**. The “nickname” you entered in Step 6 identifies the VPN Concentrator SSL certificate.

Figure 1-25: Netscape Certificates Signers list



Select a certificate, then click **Edit**, **Verify**, or **Delete**. Click **OK** when finished.

Connecting to the VPN Concentrator using HTTPS

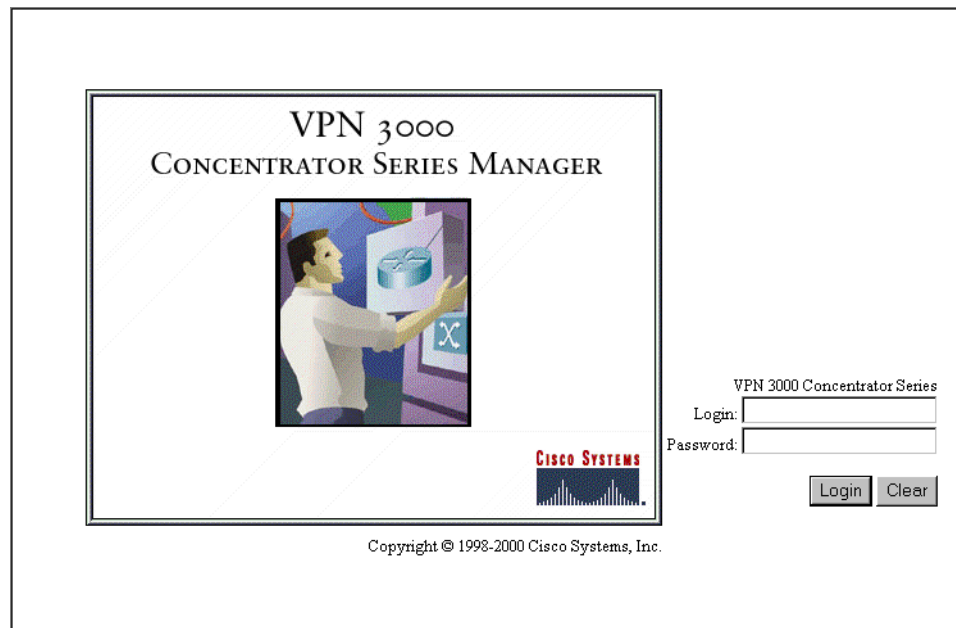
Once you have installed the VPN Concentrator SSL certificate in the browser, you can connect directly using HTTPS.

- 1 Bring up the browser.
- 2 In the browser **Address** or **Location** field, enter `https://` plus the VPN Concentrator private interface IP address; for example, `https://10.10.147.2`.

The browser displays the VPN Concentrator Manager HTTPS login screen.

A locked-padlock icon on the browser status bar indicates an HTTPS session. Also, this login screen does not include the **Install SSL Certificate** link.

Figure 1-26: VPN Concentrator Manager HTTPS login screen



Logging in the VPN Concentrator Manager

Logging in the VPN Concentrator Manager is the same for both types of connections: cleartext HTTP or secure HTTPS.

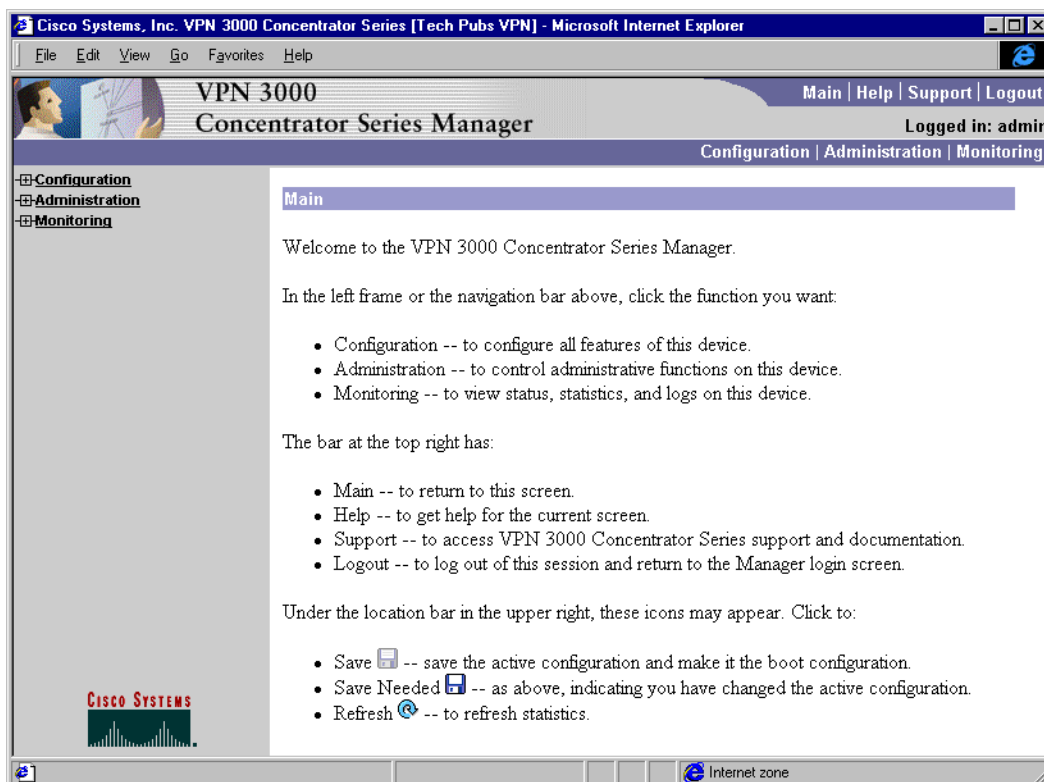
Entries are case-sensitive, so type them carefully. With Microsoft Internet Explorer, you can press the **Tab** key to move from field to field; other browsers may work differently. If you make a mistake, click the **Clear** button and start over.

The entries that follow are the factory-supplied default entries. If you have changed them, use your entries.

- 1 Click in the **Login** field and type `admin`. (*Do not press Enter.*)
- 2 Click in the **Password** field and type `admin`. (The field shows `*****`.)
- 3 Click the **Login** button.

The Manager displays the main welcome screen.

Figure 1-27: Manager Main Welcome screen



From here you can navigate the Manager using either the table of contents in the left frame, or the Manager toolbar in the top frame.

Configuring HTTP, HTTPS, and SSL parameters

HTTP, HTTPS, and SSL are enabled by default on the VPN Concentrator, and they are configured with recommended parameters that should suit most administration tasks and security requirements.

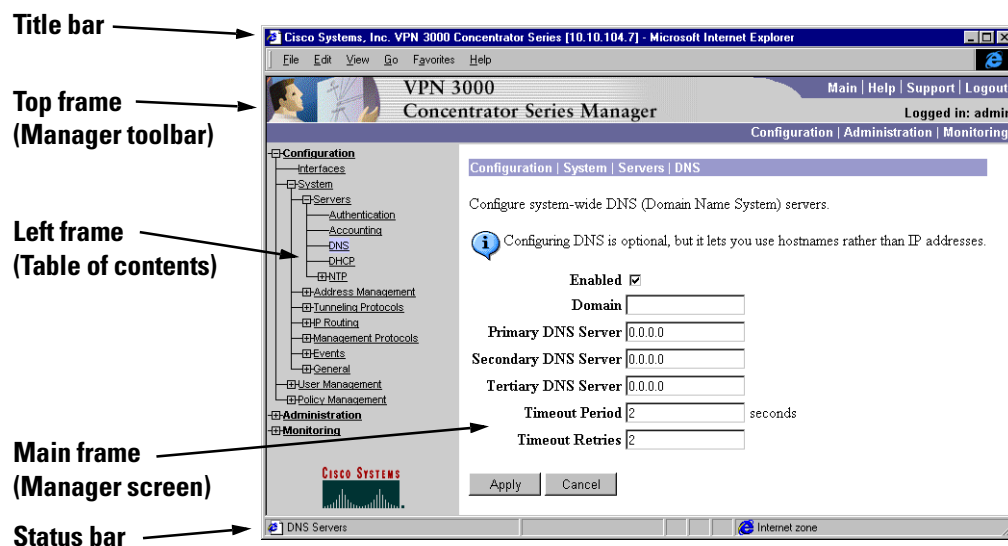
To configure HTTP and HTTPS parameters, see the **Configuration | System | Management Protocols | HTTP/HTTPS** screen.

To configure SSL parameters, see the **Configuration | System | Management Protocols | SSL** screen.

Understanding the VPN Concentrator Manager window

The VPN Concentrator Manager window on your browser consists of three frames — top, left, and main — and it provides helpful messages and tips as you move the mouse pointer over window items. The title bar and status bar also provide useful information.

Figure 1-28: VPN Concentrator Manager window.



Title bar

The title bar at the top of the browser window includes the VPN Concentrator device name or IP address in brackets; e.g., [10.10.104.7].

Status bar

The status bar at the bottom of the browser window displays explanatory messages for selected items and Manager activity.

Mouse pointer and tips

As you move the mouse pointer over an active area, the pointer changes shape and icons change color. A description also appears in the status bar area. If you momentarily rest the pointer on an icon, a descriptive tip appears for that icon.

Top frame (Manager toolbar)

The Manager toolbar in the top frame provides quick access to Manager features.

Main tab **Main**

Click to go to the main Manager screen, and to close all subordinate sections and titles in the left frame.

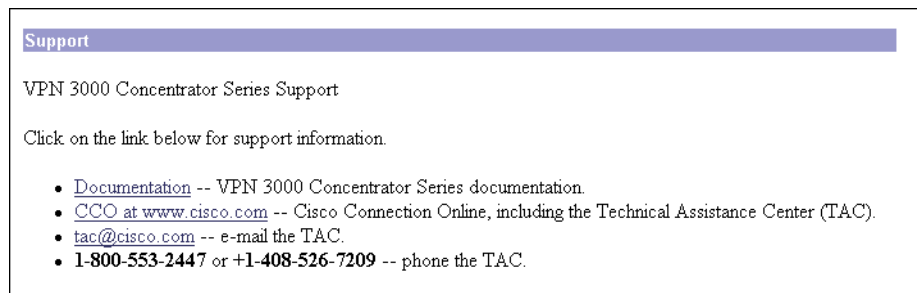
Help tab **Help**

Click to open context-sensitive online help. Help opens in a separate browser window that you can move or resize as you wish. Close the help window when you are finished.

Support tab **Support**

Click to open a Manager screen with links to Cisco support and documentation resources.

Figure 1-29: Support screen



Documentation

Click this link to open a browser window on the Cisco Technical Documentation Web page for Virtual Private Networks. That page has links to VPN 3000 Concentrator Series documentation in PDF format. (To view the PDF files, you need Adobe® Acrobat® Reader 3.0 or later, and version 4.0 is included on the VPN 3000 Concentrator Series software CD-ROM.) When you finish, close the documentation browser window and return to the Manager.

CCO at www.cisco.com

Click this link to open a browser window on the main Cisco Web page, Cisco Connection Online (CCO). From that page, you can browse to all Cisco resources, including the Technical Assistance Center (TAC). When you finish, close the CCO browser window and return to the Manager.

tac@cisco.com

Click this link to open your configured email application and compose an email message to Cisco's Technical Assistance Center (TAC). When you finish, the application closes and returns to this **Support** screen.

Logout tab

Click to log out of the Manager and return to the login screen.

Logged in: [username]

The administrator username you used to log in to this Manager session.

Configuration tab

Click to go to the main Configuration screen, to open the first level of subordinate Configuration pages in the left frame if they are not already open, and to close Administration or Monitoring pages in the left frame.

Administration tab

Click to go to the main Administration screen, to open the first level of subordinate Administration pages in the left frame if they are not already open, and to close Configuration or Monitoring pages in the left frame.

Monitoring tab

Click to go to the main Monitoring screen, to open the first level of subordinate Monitoring pages in the left frame if they are not already open, and to close Configuration or Administration pages in the left frame.

Save

Click to save the active configuration and make it the boot configuration. In this state, the reminder indicates that the active configuration is the same as the boot configuration, but you can save it anyway. When you change the configuration, the reminder changes to **Save Needed**.

Save Needed

This reminder indicates that you have changed the active configuration. Click to save the active configuration and make it the boot configuration. As you make configuration entries, they take effect immediately and are included in the active, or running, configuration. *However, if you reboot the VPN Concentrator without **saving** the active configuration, any configuration changes are lost.* Clicking this reminder saves the active configuration as the boot configuration and restores the **Save** reminder.

Refresh

Click to refresh (update) the screen contents on screens where it appears (mostly in the Monitoring section). The date and time above this reminder indicate when the screen was last updated.



Click the Cisco Systems logo to open a browser and go to the Cisco web site, www.cisco.com.

Left frame (Table of contents)

The left frame provides a table of contents to Manager screens. The table of contents uses the familiar Windows Explorer metaphor of collapsed and expanded entries.

Main section titles (Configuration, Administration, Monitoring)

Click a title to open subordinate sections and titles, and to go to that Manager screen in the main frame.

Closed or collapsed

Click the closed / collapsed icon to open subordinate sections and titles. Clicking this icon does not change the screen in the main frame.

Open or expanded

Click the open / expanded icon to close subordinate sections and titles. Clicking this icon does not change the screen in the main frame.

Main frame (Manager screen)

The main frame displays the current VPN Concentrator Manager screen.

Many screens include a bullet list of links and descriptions of subordinate sections and titles. You can click a link to go to that Manager screen and open subordinate sections and titles in the table of contents.

Organization of the VPN Concentrator Manager

The VPN Concentrator Manager consists of three major sections and many subsections:

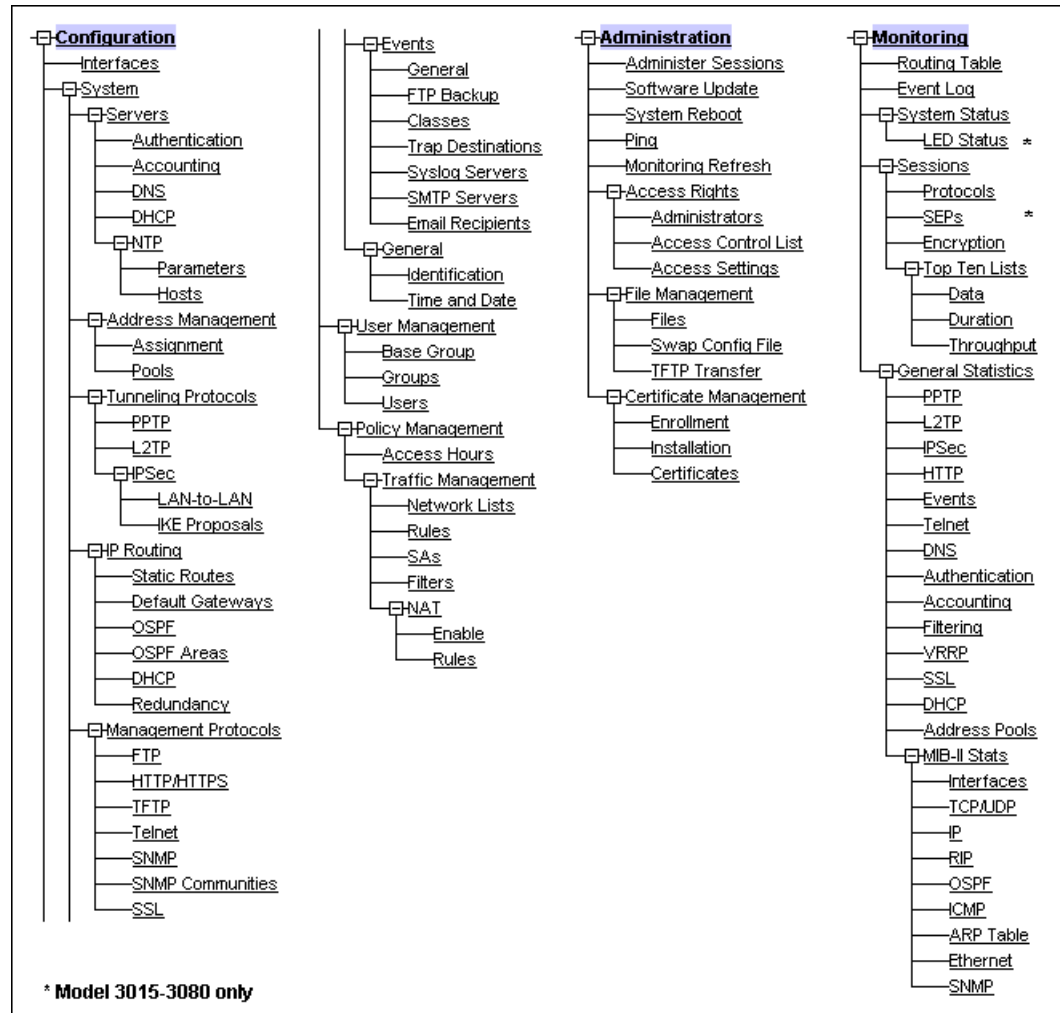
- **Configuration:** setting all the parameters for the VPN Concentrator that govern its use and functionality as a VPN device:
 - **Interfaces:** Ethernet, WAN, and power supply interface parameters.
 - **System:** parameters for system-wide functions such as server access, address management, tunneling protocols, IP routing, built-in management servers, event handling, and system identification.
 - **User Management:** attributes for groups and users that determine their access to and use of the VPN.
 - **Policy Management:** policies that control access times and data traffic through the VPN via filters, rules, and IPSec Security Associations.
- **Administration:** managing higher level functions that keep the VPN Concentrator operational and secure, such as who is allowed to configure the system, what software runs on it, and managing its digital certificates.
- **Monitoring:** viewing routing tables, event logs, system LEDs and status, data on user sessions, and statistics for protocols and system functions.

This manual covers all these topics. For Quick Configuration, see the *VPN 3000 Concentrator Series Getting Started* manual.

Navigating the VPN Concentrator Manager

Your primary tool for navigating the VPN Concentrator Manager is the table of contents in the left frame. Figure 1-30 shows all its entries, completely expanded. (The figure shows the frame in multiple columns, but the actual frame is a single column. Use the scroll controls to move up and down the frame.)

Figure 1-30: Complete Manager Table of Contents



End of Chapter



Configuration

Configuring the VPN Concentrator means setting all the parameters that govern its use and functionality as a VPN device.

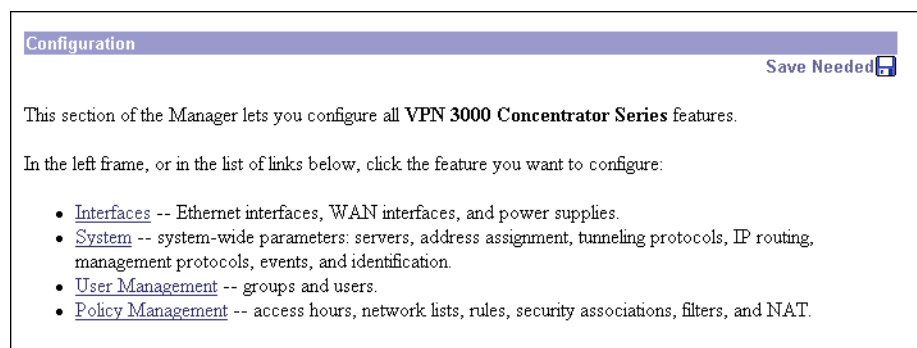
Cisco supplies default parameters that cover typical installations and uses; and once you supply minimal parameters in Quick Configuration, the system is operational. But to tailor the system to your needs, and to provide an appropriate level of system security, you should configure the system in detail.

Configuration

This section of the Manager lets you configure all VPN Concentrator features and functions.

- **Interfaces:** parameters specific to the Ethernet interfaces: public, private, and external; WAN interfaces: ports A and B; plus power supply and voltage sensor alarms.
- **System:** parameters for system-wide functions: server access, address assignment, tunneling protocols, IP routing, built-in management servers, system events, and system identification.
- **User Management:** attributes for groups and users that determine their access to and use of the VPN.
- **Policy Management:** policies that control data traffic through the VPN via filters, rules, and IPSec Security Associations; network lists; access times; and NAT.

Figure 2-1: Configuration screen



See the appropriate chapter in this manual for each section of the Manager. Online help is available for all sections.

End of Chapter



Interfaces

This section of the VPN 3000 Concentrator Series Manager applies primarily to Ethernet and WAN network interfaces. Here you configure functions that are interface-specific, rather than system-wide. There is also a screen to configure power supply and voltage sensor alarms.

Typically, you configure at least two network interfaces for the VPN Concentrator to operate as a VPN device: usually the Ethernet 1 (Private) interface and either the Ethernet 2 (Public) interface or a WAN interface port. If you used Quick Configuration as described in the *VPN 3000 Concentrator Series Getting Started* manual, the system supplied many default parameters for the interfaces. Here you can configure them explicitly.

The VPN Concentrator uses filters to control data traffic through the system; see **Configuration | Policy Management | Traffic Management**. You apply filters both to interfaces and to groups and users. Group and user filters govern *tunneled group* and *user* data traffic; interface filters govern *all* data traffic.

Network interfaces usually connect to a router that routes data traffic to other networks. The VPN Concentrator includes IP routing functions: static routes, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First). You configure RIP and interface-specific OSPF here. You configure static routes, the default gateway, and system-wide OSPF in the IP Router section; see the **Configuration | System | IP Routing** screens.

RIP and OSPF are routing protocols that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports RIP versions 1 and 2, and OSPF version 2. You can enable both RIP and OSPF on an interface.

Filter settings override RIP and OSPF settings on an interface; therefore, be sure settings in filter rules are consistent with RIP and OSPF use. For example, if you intend to use RIP, be sure you apply a filter rule that forwards TCP/UDP packets with the RIP port configured.

Configuration | Interfaces

This section lets you configure the three VPN Concentrator Ethernet interface modules and, if present, two WAN module interface ports. You can also configure alarm thresholds for the power supply modules.

Model 3005 comes with two Ethernet interfaces. Models 3015–3080 come with three Ethernet interfaces. Optionally, all models can have a WAN interface module installed, with two T1/E1 WAN interface ports.

- Ethernet 1 (Private) is the interface to your private network (internal LAN).
- Ethernet 2 (Public) is the interface to the public network.
- Ethernet 3 (External) is the interface to an additional LAN (Models 3015–3080 only).
- WAN interface Port A is a T1/E1 interface, usually to the public network.
- WAN interface Port B is a T1/E1 interface, usually to the public network.

Configuring an Ethernet interface includes supplying an IP address, applying a traffic-management filter, setting speed and transmission mode, and configuring RIP and OSPF routing protocols.

Configuring a WAN interface includes selecting the interface type (T1 or E1), supplying an IP address, applying a traffic-management filter, configuring RIP and OSPF routing protocols, and configuring T1- or E1-specific parameters. You can also enable PPP Multilink.

If you connect to a WAN via an ISP, configure that connection on Port A. You can use Port B to provide PPP Multilink for increased bandwidth. You cannot connect Port B to a WAN from a different ISP. If you connect to private WANs, you can configure independent WAN connections on Port A and Port B.

Note: Interface settings take effect as soon as you apply them. If the system is in active use, changes may affect tunnel traffic.

The table shows all installed interfaces and their status.

Figure 3-1: Configuration | Interfaces screen

Model 3005

Configuration | Interfaces Save Needed

This section lets you configure the VPN 3000 Concentrator Series network interfaces.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	100.200.147.5	255.0.0.0
Ethernet 2 (Public)	Not Configured		

- [Power Supply](#)

Model 3015–3080

Configuration | Interfaces Save Needed

This section lets you configure the VPN 3000 Concentrator Series network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	100.200.147.2	255.0.0.0
Ethernet 2 (Public)	DOWN	192.168.12.34	255.255.255.0
Ethernet 3 (External)	Not Configured		
WAN Interface in slot 2, port A	T1/Red	192.168.34.56	255.255.255.0
WAN Interface in slot 2, port B	Not Configured		

- [Power Supplies](#)

To configure a module, either click the appropriate link in the status table; or use the mouse pointer to select the module on the back-panel image, and click anywhere in the highlighted area.

Interface

The VPN Concentrator interface installed in the system. To configure an interface, click the appropriate link.

Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External)

To configure Ethernet interface parameters, click the appropriate highlighted link in the table or click in a highlighted module on the back-panel image. See [Configuration | Interfaces | Ethernet 1 2 3](#).

WAN Interface in slot N, Port A B

To configure parameters for a specific WAN interface port, click the appropriate highlighted link in the table. If you are configuring the WAN interface for the first time, see the [Configuration | Interfaces | WAN Card in Slot N | Port A B | Select T1/E1](#) screen. Otherwise, see the [Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1](#) screen.

Status

The operational status of this interface. If configured, the WAN interface status includes a prefix if PPP Multilink is enabled, and the interface type (T1 or E1).

`Up` = (Green) Configured, enabled, and operational; ready to pass data traffic.

`Down` = (Red) Configured but disabled or disconnected.

`Testing` = In test mode; no regular data traffic can pass.

`Dormant` = (Red) Configured and enabled but waiting for an external action, such as an incoming connection.

`Not Present` = (Red) Missing hardware components.

`Lower Layer Down` = (Red) Not operational because a lower-layer interface is down.

`Unknown` = (Red) Not configured or not able to determine status.

`Not Configured` = Present but not configured.

`Red` = (Red) (WAN only.) Red alarm: Line has lost synchronization or signal. This alarm indicates out of frame errors or a mismatched framing format, or a disconnected line.

`Blue` = (Blue) (WAN only.) Blue alarm: A problem on the receive path is causing the line to lose the remote signal. This alarm indicates a problem in the data bit stream.

`Yellow` = (Yellow) (WAN only.) Yellow alarm: A problem on the transmit side (the remote side of the connection has detected a problem with this line).

`Loopback` = (WAN only.) Line is in loopback state.

`IP Address Not Configured` = (WAN only) Interface port that was previously configured for PPP Multilink and no longer has an IP address. To connect this port to a WAN, you must supply an IP address.

IP Address

The IP address configured on this interface.

Subnet Mask

The subnet mask configured on this interface.

Power Supplies

To configure alarm thresholds on system power supplies, click the appropriate highlighted link or click in a highlighted power supply module in the back-panel image and see [Configuration | Interfaces | Power](#).

Ethernet 1 (Private), Ethernet 2 (Public), Ethernet 3 (External) module in back-panel image

To configure Ethernet interface parameters, click the appropriate highlighted Ethernet module in the back-panel image and see [Configuration | Interfaces | Ethernet 1 2 3](#).

WAN Card Slot N module in back-panel image

To configure the WAN interface card, click the highlighted WAN card module in the back-panel image, and see [Configuration | Interfaces | WAN Card in Slot N](#).

Configuration | Interfaces | Power

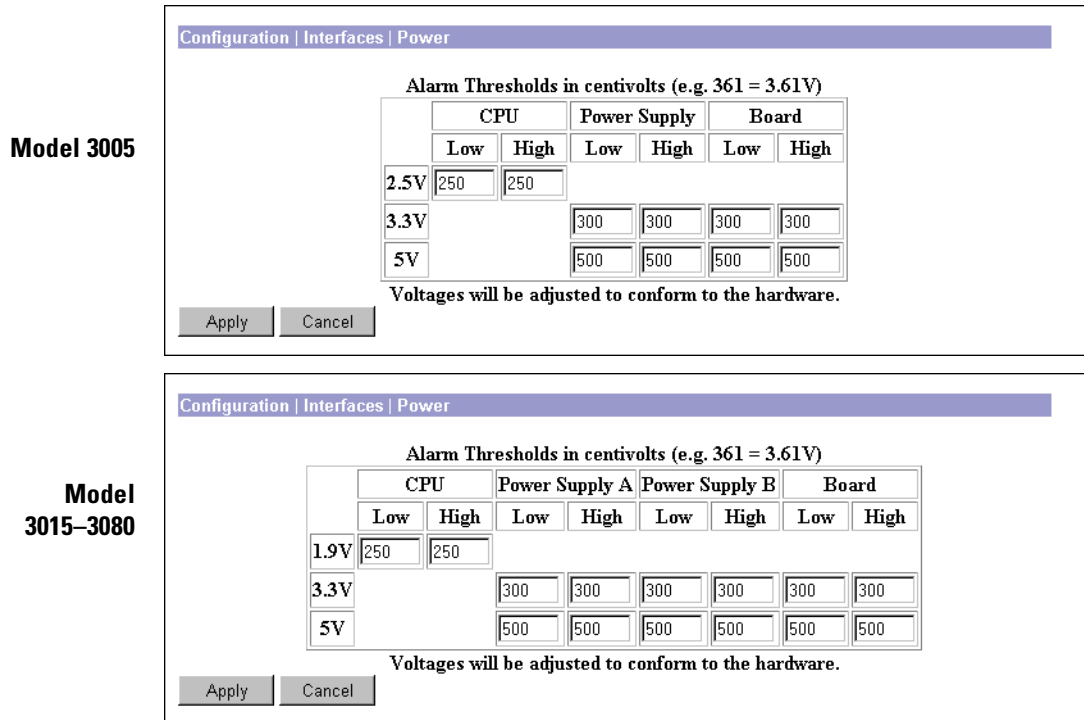
This screen lets you configure alarm thresholds for voltages in the system power supplies, CPU, and main circuit board.

On this screen, you set high and low thresholds for the voltages. When the system detects a voltage outside a threshold value, it generates a `HARDWAREMON` (hardware monitoring) event (see [Configuration | System | Events](#)). If a power supply is faulty, the appropriate **Power Supply** LED on the front panel is amber.

Caution: If a voltage generates an alarm, shut down the system in an orderly way and contact Cisco support. *Operating the system with out-of-range voltages, especially if they exceed the high threshold, may cause permanent damage.*

You can view system voltages and status on the [Monitor | System Status | Power](#) screen.

Figure 3-2: Configuration | Interfaces | Power screen



Alarm Thresholds

The fields show default values for alarm thresholds in centivolts; e.g., 361 = 3.61 volts. Enter or edit these values as desired.

The hardware sets voltage thresholds in increments that may not match an entered value. The fields show the actual thresholds, and the values may differ from your entries.

CPU

High and low thresholds for the voltage sensors on the CPU chip. The value is system dependent, either 2.5 or 1.9 volts.

Power Supply A, B

High and low thresholds for the 3.3- and 5-volt outputs from the power supplies. You can enter values for the second power supply on Models 3015-3080 even if it is not installed.

Board

High and low thresholds for the 3.3- and 5-volt sensors on the main circuit board.

Apply / Cancel

To apply your settings to the system and include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | Interfaces** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Interfaces** screen.

Configuration | Interfaces | Ethernet 1 2 3

This screen lets you configure parameters for the Ethernet interface you selected. It displays the current parameters, if any.

Configuring an Ethernet interface includes supplying an IP address, identifying it as a public interface, applying a traffic-management filter, setting speed and transmission mode, and configuring RIP and OSPF routing protocols.

To apply a custom filter, you must configure the filter first; see **Configuration | Policy Management | Traffic Management**.


Caution: If you modify any parameters of the interface that you are currently using to connect to the VPN Concentrator, you will break the connection, and you will have to restart the Manager from the login screen.

Using the tabs

This screen includes three tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Apply** or **Cancel**.

Figure 3-3: Configuration | Interfaces | Ethernet 1 2 3 screen, General tab

Configuration | Interfaces | Ethernet 1

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General RIP OSPF

General Parameters		
Attribute	Value	Description
Enabled	<input checked="" type="checkbox"/>	Check to enable this interface.
IP Address	100.200.147.10	Enter the IP address for this interface.
Subnet Mask	255.0.0.0	Enter the subnet mask for this interface.
Public Interface	<input type="checkbox"/>	Check to make this interface a "public" interface.
MAC Address	00.01.02.3A.93.FC	The MAC address for this interface.
Filter	—None—	Select the filter for this interface.
Speed	10/100 auto	Select the speed for this interface.
Duplex	Auto	Select the duplex mode for this interface.

Apply Cancel

General Parameters tab

This tab lets you configure general interface parameters: IP address, subnet mask, public interface status, filter, speed, and transmission mode.

Enabled

To make the interface functional and online, check **Enabled**. If not enabled, the interface is offline; this state lets you retain or change its configuration parameters while it is offline.

If the interface is configured but disabled (offline), the appropriate **Ethernet Link Status** LED blinks green on the VPN Concentrator front panel.

IP Address

Enter the IP address for this interface, using dotted decimal notation (e.g., 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (e.g., 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

Public Interface

To make this interface a public interface, check the box. A public interface is an interface to a public network, such as the Internet. You must configure a public interface before you can configure NAT and

IPSec LAN-to-LAN, for example. You should designate only one VPN Concentrator interface as a public interface.

MAC Address

This is the unique hardware MAC (Medium Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Filter

The filter governs the handling of data packets through this interface: whether to forward or drop, according to configured criteria. Cisco supplies three default filters that you can modify and use with the VPN Concentrator. You can configure filters on the **Configuration | Policy Management | Traffic Management** screens.

Click the drop-down menu button and select the filter to apply to this interface:

- 1. Private (Default)** = Allow all packets except source-routed IP packets. Cisco supplies this default filter for Ethernet 1, but it is not selected by default.
 - 2. Public (Default)** = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. Cisco supplies this default filter for Ethernet 2, and it is selected by default for Ethernet 2.
 - 3. External (Default)** = No rules applied to this filter. Drop all packets. Cisco supplies this default filter for Ethernet 3, but it is not selected by default.
- None– = No filter applied to the interface, which means there are no restrictions on data packets. This is the default selection for Ethernet 1 and 3.

Other filters that you have configured also appear in this menu.

Speed

Click the drop-down menu button and select the interface speed:

- 10 Mbps** = Fix the speed at 10 megabits per second (10Base-T networks)
- 100 Mbps** = Fix the speed at 100 megabits per second (100Base-T networks)
- 10/100 auto** = Let the VPN Concentrator automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Duplex

Click the drop-down menu button and select the interface transmission mode:

- Auto** = Let the VPN Concentrator automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.
- Full-Duplex** = Fix the transmission mode as full duplex: transmission in both directions at the same time.
- Half-Duplex** = Fix the transmission mode as half duplex: transmission in only one direction at a time.

Figure 3-4: Configuration | Interfaces | Ethernet 1 2 3 screen, RIP tab

Configuration | Interfaces | Ethernet 1

Warning: You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General **RIP** OSPF

RIP Parameters		
Attribute	Value	Description
Inbound RIP	RIPv2/v1	Select the method of inbound RIP processing for this interface.
Outbound RIP	Disabled	Select the method of outbound RIP processing for this interface.

Apply Cancel

RIP Parameters tab

RIP is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. RIP uses distance-vector routing algorithms, and it is an older protocol that generates more network traffic than OSPF. The VPN Concentrator includes IP routing functions that support RIP versions 1 and 2. Many private networks with simple topologies still use RIPv1, although it lacks security features. RIPv2 is generally considered the preferred version; it includes functions for authenticating other routers, for example.

To use the **Network Autodiscovery** feature in IPsec LAN-to-LAN configuration, or to use the automatic list generation feature in Network Lists, you must enable **Inbound RIPv2/v1** on Ethernet 1. (It is enabled by default.)

Inbound RIP

This parameter applies to RIP messages coming into the VPN Concentrator. It configures the system to listen for RIP messages on this interface.

Click the drop-down menu button and select the inbound RIP function:

Disabled = No inbound RIP functions; i.e., the system does not listen for any RIP messages on this interface (default for Ethernet 2 and 3).

RIPv1 Only = Listen for and interpret only RIPv1 messages on this interface.

RIPv2 Only = Listen for and interpret only RIPv2 messages on this interface.

RIPv2/v1 = Listen for and interpret either RIPv1 or RIPv2 messages on this interface (default for Ethernet 1).

Outbound RIP

This parameter applies to RIP messages going out of the VPN Concentrator; that is, it configures the system to send RIP messages on this interface.

Click the drop-down menu button and select the outbound RIP function:

Disabled = No outbound RIP functions; i.e., the system does not send any RIP messages on this interface (default).


RIPv1 Only = Send only RIPv1 messages on this interface.

RIPv2 Only = Send only RIPv2 messages on this interface.

RIPv2/v1 compatible = Send RIPv2 messages that are compatible with RIPv1 on this interface.

Figure 3-5: Configuration | Interfaces | Ethernet 1 2 3 screen, OSPF tab

Configuration | Interfaces | Ethernet 1

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General
RIP
OSPF

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input type="checkbox"/>	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None <input type="button" value="v"/>	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when <i>Simple Password</i> or <i>MD5</i> is selected above.

OSPF Parameters tab

OSPF is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. OSPF uses link-state routing algorithms, and it is a newer protocol than RIP. It generates less network traffic and generally provides faster routing updates, but it requires more processing power than RIP. The VPN Concentrator includes IP routing functions that support OSPF version 2 (RFC 2328).

OSPF involves interface-specific parameters that you configure here, and system-wide parameters that you configure on the **Configuration | System | IP Routing** screens.

OSPF Enabled

To enable OSPF routing on this interface, check the box. (By default it is not checked.)

To activate the OSPF system, you must also configure and enable OSPF on the **Configuration | System | IP Routing | OSPF** screen.

OSPF Area ID

The area ID identifies the subnet area within the OSPF Autonomous System or domain. Routers within an area have identical link-state databases. While its format is that of a dotted decimal IP address, the ID is only an identifier and not an address.

The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers, which are the routers connected to multiple areas.

Enter the area ID in the field, using IP address format in dotted decimal notation (e.g., 10.10.0.0). The default entry is 0.0.0.0, the backbone. Your entry also appears in the **OSPF Area** list on the **Configuration | System | IP Routing | OSPF Areas** screen.

OSPF Priority

This entry assigns a priority to the OSPF router on this interface. OSPF routers on a network elect one to be the Designated Router, which has the master routing database and performs other administrative functions. In case of a tie, the router with the highest priority number wins. A 0 entry means this router is ineligible to become the Designated Router.

Enter the priority as a number from 0 to 255. The default is 1.

OSPF Metric

This entry is the metric, or cost, of the OSPF router on this interface. The cost determines preferred routing through the network, with the lowest cost being the most desirable.

Enter the metric as a number from 1 to 65535. The default is 1.

OSPF Retransmit Interval

This entry is the number of seconds between OSPF Link State Advertisements (LSAs) from this interface, which are messages that the router sends to describe its current state.

Enter the interval as a number from 0 to 3600 seconds. The default is 5 seconds, which is a typical value for LANs.

OSPF Hello Interval

This entry is the number of seconds between Hello packets that the router sends to announce its presence, join the OSPF routing area, and maintain neighbor relationships. This interval must be the same for all routers on a common network.

Enter the interval as a number from 1 to 65535 seconds. The default is 10 seconds, which is a typical value for LANs.

OSPF Dead Interval

This entry is the number of seconds for the OSPF router to wait before it declares that a neighboring router is out of service, after the router no longer sees the neighbor's Hello packets. This interval should be some multiple of the Hello Interval, and it must be the same for all routers on a common network.

Enter the interval as a number from 0 to 65535 seconds. The default is 40 seconds, which is a typical value for LANs.

OSPF Transit Delay

This entry is the estimated number of seconds it takes to transmit a link state update packet over this interface, and it should include both the transmission and propagation delays of the interface. This delay must be the same for all routers on a common network.

Enter the delay as a number from 0 to 3600 seconds. The default is 1 second, which is a typical value for LANs.

OSPF Authentication

This parameter sets the authentication method for OSPF protocol messages. OSPF messages can be authenticated so that only trusted routers can route messages within the domain. This authentication method must be the same for all routers on a common network.

Click the drop-down menu button and select the authentication method:

None = No authentication. OSPF messages are not authenticated (default).

Simple Password = Use a clear-text password for authentication. This password must be the same for all routers on a common network. If you select this method, enter the password in the **OSPF Password** field below.

MD5 = Use the MD5 hashing algorithm with a shared key to generate an encrypted message digest for authentication. This key must be the same for all routers on a common network. If you select this method, enter the key in the **OSPF Password** field below.

OSPF Password

If you selected **Simple Password** or **MD5** for **OSPF Authentication** above, enter the appropriate password or key in this field. Otherwise, leave the field blank.

For **Simple Password** authentication, enter the common password. Maximum 8 characters. The Manager displays your entry in clear text.

For **MD5** authentication, enter the shared key. Maximum 8 characters. The Manager displays your entry in clear text.

Apply / Cancel

To apply your settings to this interface and include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | Interfaces** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

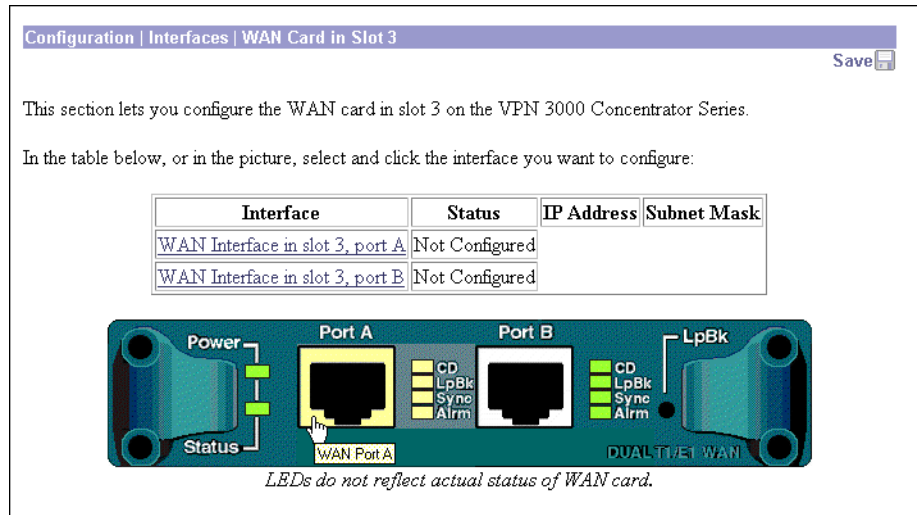
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Interfaces** screen.

Configuration | Interfaces | WAN Card in Slot N

The Manager displays this screen when you click the WAN module in the back-panel image on the **Configuration | Interfaces** screen. The table shows the status of the WAN module interface ports, and from there you can choose a port to configure.

Note that the LEDs on this screen do not show actual WAN card LED states.

Figure 3-6: Configuration | Interfaces | WAN Card in Slot N screen



To configure an interface port, either click the link in the status table, or select and click the highlighted port in the WAN module image. If you are configuring the WAN interface for the first time, see the **Configuration | Interfaces | WAN Card in Slot N | Port A B | Select T1/E1** screen. Otherwise, see the **Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1** screen.

Interface

The interface port on this WAN module.

Status

The operational status of this interface. If the interface is configured, the status includes a prefix if PPP Multilink is enabled, and the interface type (T1 or E1).

Up = (Green) Configured, enabled, and operational; ready to pass data traffic.

Down = (Red) Configured but disabled or disconnected.

Testing = In test mode; no regular data traffic can pass.

Dormant = (Red) Configured and enabled but waiting for an external action, such as an incoming connection.

Not Present = (Red) Missing hardware components.

Lower Layer Down = (Red) Not operational because a lower-layer interface is down.

Unknown = (Red) Not configured or not able to determine status.

Not Configured = Present but not configured.

Red = (Red) Red alarm: Line has lost synchronization or signal. This alarm indicates out of frame errors or a mismatched framing format, or a disconnected line.

Blue = (Blue) Blue alarm: A problem on the receive path is causing the line to lose the remote signal. This alarm indicates a problem in the data bit stream.

Yellow = (Yellow) Yellow alarm: A problem on the transmit side (the remote side of the connection has detected a problem with this line).

Loopback = Line is in loopback state.

IP Address Not Configured = (WAN only) Interface port that was previously configured for PPP Multilink and no longer has an IP address. To connect this port to a WAN, you must supply an IP address.

IP Address

The IP address configured on this interface port.

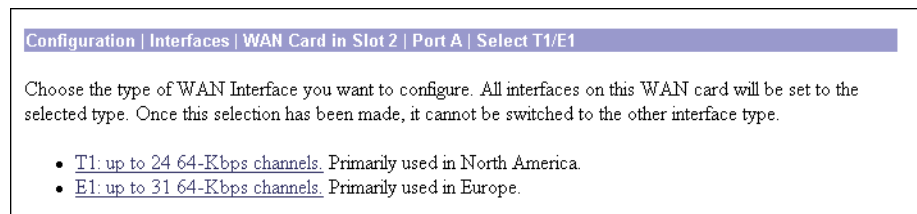
Subnet Mask

The subnet mask configured on this interface port.

Configuration | Interfaces | WAN Card in Slot N | Port A B | Select T1/E1

This screen lets you choose either T1 or E1 interface type for the WAN module, and it appears only when you configure the WAN module for the first time. Once chosen, the type is permanent and applies to both ports (interfaces) on the module.

Figure 3-7: Configuration | Interfaces | WAN Card in Slot N | Port A B | Select T1/E1 screen



Click the link to choose the desired interface type.

T1: up to 24 64-Kbps channels

The T1 interface conforms to North American Digital Hierarchy standards, with up to 24 64-Kbps channels for a maximum of 1536 Kbps.

When you click this link, the Manager opens the **Configuration | Interfaces | WAN Card in Slot N | Port A B as T1** screen, which lets you configure T1 parameters.

E1: up to 31 64-Kbps channels

The E1 interface conforms to European Digital Hierarchy standards, with up to 31 64-Kbps channels for a maximum of 1984 Kbps.

When you click this link, the Manager opens the **Configuration | Interfaces | WAN Card in Slot N | Port A B as E1** screen, which lets you configure E1 parameters.

Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1

This screen lets you configure parameters for the WAN interface port you selected. The Dual T1/E1 WAN module for the VPN Concentrator includes two WAN interfaces, one on Port A and the other on Port B. The WAN interfaces primarily serve as a public interface to the Internet.

- If you connect to a WAN via an ISP, configure that connection on Port A. You can use Port B to provide PPP Multilink for increased bandwidth. You cannot connect Port B to a WAN from a different ISP.
- If you connect to private WANs, you can configure independent WAN connections on Port A and Port B.

The WAN module supports complete T1/E1 interfaces and fractional T1/E1 interfaces. You can select T1/E1 bandwidth by configuring specific DS0 (Digital Signal 0) channels. See the **Timeslots** parameter on the **WAN Parameters** tab.

You set the interface type (T1 or E1) on the **Configuration | Interfaces | WAN Card in Slot N | Port A B | Select T1/E1** screen. Once chosen, the type is permanent and applies to both ports (interfaces) on the module.

Configuring a WAN interface includes supplying an IP address, identifying it as a public interface, applying a traffic-management filter, configuring RIP and OSPF routing protocols, and setting T1- or E1-specific parameters to match those of your T1/E1 carrier. You can also configure PPP Multilink.

To apply a custom filter, you must configure the filter first; see **Configuration | Policy Management | Traffic Management**.

Using the tabs

This screen includes five tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Apply** or **Cancel**.

Figure 3-8: Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1 screen, IP tab

IP Parameters		
Attribute	Value	Description
Enabled	<input checked="" type="checkbox"/>	Check to enable this interface.
IP Address	<input type="text"/>	Enter the IP address for this interface.
Subnet Mask	<input type="text"/>	Enter the subnet mask for this interface.
Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
Filter	<input type="text" value="-Make copy of filter 2 (public)-"/>	Select the filter for this interface.

Apply Cancel

IP Parameters tab

This tab lets you configure IP address, subnet mask, public interface status, and filter.

Enabled

To make the WAN interface functional and online, check **Enabled**. If not enabled, the interface is offline; this state lets you retain or change its configuration parameters while it is offline.

If the WAN port is configured but disabled (offline), all four **Port** LEDs on the WAN module blink in unison.

IP Address

Enter the IP address for this interface, using dotted decimal notation (e.g., 192 . 168 . 12 . 34). Note that 0 . 0 . 0 . 0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (e.g., 255 . 255 . 255 . 0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192 . 168 . 12 . 34 is a Class C address, and the standard subnet mask is 255 . 255 . 255 . 0. You can accept this entry or change it. Note that 0 . 0 . 0 . 0 is not allowed.

Public Interface

To make this interface a public interface, check the box. (The box is checked by default.) A public interface is an interface to a public network, such as the Internet. You must configure a public interface before you can configure NAT and IPsec LAN-to-LAN, for example. You should designate only one VPN Concentrator interface as a public interface.

Filter

The filter governs the handling of data packets through this interface: whether to forward or drop, according to configured criteria. Cisco supplies three default filters that you can modify and use with the VPN Concentrator. You can configure filters on the **Configuration | Policy Management | Traffic Management** screens.

Click the drop-down menu button and select the filter to apply to this interface:

1. **Private (Default)** = Allow all packets except source-routed IP packets.
 2. **Public (Default)** = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets.
 3. **External (Default)** = No rules applied to this filter. Drop all packets.
- None**– = No filter applied to the interface, which means there are no restrictions on data packets.
- Make copy of filter 2 (public)**– = Make and apply a copy of the **2. Public (Default)** filter. The system names this filter **WAN filter n**, where **n** is the next available filter number (usually 4). It is a copy of the current **2. Public (Default)** filter with all its parameters and rules *except* any **Apply IPSec** (LAN-to-LAN) rules. See **Configuration | Policy Management | Traffic Management | Filters**.

Other filters that you have configured also appear in this menu.

We recommend that you accept the default –**Make copy of filter 2 (public)**–, especially when you initially configure this interface. You can select this option only when you initially configure this interface. If you select a different option initially and decide later to use the public filter, you must manually make a copy of the public filter and assign it to the interface.

Figure 3-9: Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1 screen, RIP tab

Configuration | Interfaces | WAN Card in slot 2 | Port A as E1

IP RIP OSPF WAN PPP

Configuration | Interfaces | WAN Card in slot 2 | Port A as T1

IP RIP OSPF WAN PPP

RIP Parameters		
Attribute	Value	Description
Inbound RIP	Disabled	Select the method of inbound RIP processing for this interface.
Outbound RIP	Disabled	Select the method of outbound RIP processing for this interface.

Apply Cancel

RIP Parameters tab

RIP is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. RIP uses distance-vector routing algorithms, and it is an older protocol that generates more network traffic than OSPF. The VPN Concentrator includes IP routing functions that support RIP versions 1 and 2. Many private networks with simple topologies still use RIPv1, although it lacks security features. RIPv2 is generally considered the preferred version; it includes functions for authenticating other routers, for example.

Inbound RIP

This parameter applies to RIP messages coming into the VPN Concentrator. It configures the system to listen for RIP messages on this interface.

Click the drop-down menu button and select the inbound RIP function:

Disabled = No inbound RIP functions; i.e., the system does not listen for any RIP messages on this interface (default).

RIPv1 Only = Listen for and interpret only RIPv1 messages on this interface.

RIPv2 Only = Listen for and interpret only RIPv2 messages on this interface.

RIPv2/v1 = Listen for and interpret either RIPv1 or RIPv2 messages on this interface.

Outbound RIP

This parameter applies to RIP messages going out of the VPN Concentrator; that is, it configures the system to send RIP messages on this interface.

Click the drop-down menu button and select the outbound RIP function:

Disabled = No outbound RIP functions; i.e., the system does not send any RIP messages on this interface (default).

RIPv1 Only = Send only RIPv1 messages on this interface.

RIPv2 Only = Send only RIPv2 messages on this interface.

RIPv2/v1 compatible = Send RIPv2 messages that are compatible with RIPv1 on this interface.

Figure 3-10: Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1 screen, OSPF tab

OSPF Parameters		
Attribute	Value	Description
OSPF Enabled	<input type="checkbox"/>	Check to enable OSPF on this interface.
OSPF Area ID	0.0.0.0	Enter the OSPF Area ID for this interface. The format is the same as an IP address.
OSPF Priority	1	Enter the OSPF Priority for this interface.
OSPF Metric	1	Enter the OSPF Metric for this interface.
OSPF Retransmit Interval	5	Enter the OSPF Retransmit Interval for this interface.
OSPF Hello Interval	10	Enter the OSPF Hello Interval for this interface.
OSPF Dead Interval	40	Enter the OSPF Dead Interval for this interface.
OSPF Transit Delay	1	Enter the OSPF Transit Delay for this interface.
OSPF Authentication	None	Select the OSPF Authentication method to use.
OSPF Password		Enter the OSPF Password when <i>Simple Password</i> is selected above.

Apply Cancel

OSPF Parameters tab

OSPF is a routing protocol that routers use for messages to other routers, to determine network connectivity, status, and optimum paths for sending data traffic. OSPF uses link-state routing algorithms, and it is a newer protocol than RIP. It generates less network traffic and generally provides faster routing updates, but it requires more processing power than RIP. The VPN Concentrator includes IP routing functions that support OSPF version 2 (RFC 2328).

OSPF involves interface-specific parameters that you configure here, and system-wide parameters that you configure on the **Configuration | System | IP Routing** screens.

OSPF Enabled

To enable OSPF routing on this interface, check the box. (By default it is not checked.)

To activate the OSPF system, you must also configure and enable OSPF on the **Configuration | System | IP Routing | OSPF** screen.

OSPF Area ID

The area ID identifies the subnet area within the OSPF Autonomous System or domain. Routers within an area have identical link-state databases. While its format is that of a dotted decimal IP address, the ID is only an identifier and not an address.

The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers, which are the routers connected to multiple areas.

Enter the area ID in the field, using IP address format in dotted decimal notation (e.g., 10.10.0.0). The default entry is 0.0.0.0, the backbone. Your entry also appears in the **OSPF Area** list on the **Configuration | System | IP Routing | OSPF Areas** screen.

OSPF Priority

This entry assigns a priority to the OSPF router on this interface. OSPF routers on a network elect one to be the Designated Router, which has the master routing database and performs other administrative functions. In case of a tie, the router with the highest priority number wins. A 0 entry means this router is ineligible to become the Designated Router.

Enter the priority as a number from 0 to 255. The default is 1.

OSPF Metric

This entry is the metric, or cost, of the OSPF router on this interface. The cost determines preferred routing through the network, with the lowest cost being the most desirable.

Enter the metric as a number from 1 to 65535. The default is 1.

OSPF Retransmit Interval

This entry is the number of seconds between OSPF Link State Advertisements (LSAs) from this interface, which are messages that the router sends to describe its current state.

Enter the interval as a number from 0 to 3600 seconds. The default is 5 seconds, which is a typical value.

OSPF Hello Interval

This entry is the number of seconds between Hello packets that the router sends to announce its presence, join the OSPF routing area, and maintain neighbor relationships. This interval must be the same for all routers on a common network.

Enter the interval as a number from 1 to 65535 seconds. The default is 10 seconds, which is a typical value.

OSPF Dead Interval

This entry is the number of seconds for the OSPF router to wait before it declares that a neighboring router is out of service, after the router no longer sees the neighbor's Hello packets. This interval should be some multiple of the Hello Interval, and it must be the same for all routers on a common network.

Enter the interval as a number from 0 to 65535 seconds. The default is 40 seconds, which is a typical value.

OSPF Transit Delay

This entry is the estimated number of seconds it takes to transmit a link state update packet over this interface, and it should include both the transmission and propagation delays of the interface. This delay must be the same for all routers on a common network.

Enter the delay as a number from 0 to 3600 seconds. The default is 1 second, which is a typical value.

OSPF Authentication

This parameter sets the authentication method for OSPF protocol messages. OSPF messages can be authenticated so that only trusted routers can route messages within the domain. This authentication method must be the same for all routers on a common network.

Click the drop-down menu button and select the authentication method:

None = No authentication. OSPF messages are not authenticated (default).

Simple Password = Use a clear-text password for authentication. This password must be the same for all routers on a common network. If you select this method, enter the password in the **OSPF Password** field below.

MD5 = Use the MD5 hashing algorithm with a shared key to generate an encrypted message digest for authentication. This key must be the same for all routers on a common network. If you select this method, enter the key in the **OSPF Password** field below.

OSPF Password

If you selected **Simple Password** or **MD5** for **OSPF Authentication** above, enter the appropriate password or key in this field. Otherwise, leave the field blank.

For **Simple Password** authentication, enter the common password. Maximum 8 characters. The Manager displays your entry in clear text.

For **MD5** authentication, enter the shared key. Maximum 8 characters. The Manager displays your entry in clear text.

Figure 3-11: Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1 screen, WAN tab

Configuration | Interfaces | WAN Card in slot 3 | Port A as E1

IP RIP OSPF **WAN** PPP

Configuration | Interfaces | WAN Card in slot 2 | Port A as T1

IP RIP OSPF **WAN** PPP

WAN Parameters		
Attribute	Value	Description
Line Coding	B8ZS	Select the line coding for this WAN port.
Line Framing	ESF	Select the line framing for this WAN port.
Buildout	-0.0 dB	Select the buildout for this WAN port.
Clock Source	Line	Select the clock source for this WAN port.
Data Inversion	<input type="checkbox"/>	Check to invert the data on this WAN port.
Loopback	None	Select the loopback configuration for this WAN port.
Timeslots	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 19 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 20 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 15 <input checked="" type="checkbox"/> 21 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 16 <input checked="" type="checkbox"/> 22 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 17 <input checked="" type="checkbox"/> 23 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24	Check the timeslots for this WAN port. Each timeslot is 64Kbps. Currently: 1536 Kbps. <input type="button" value="Clear All"/> <input type="button" value="Set All"/>

WAN Parameters tab

This tab lets you configure T1/E1 parameters: line coding, line framing, line buildout, clock source, data inversion, loopback mode, and timeslots.

Line Coding

A T1/E1 line uses a bipolar format for generating signals, with alternating plus and minus pulses. The line codes maintain synchronization on the line. To set the correct line code, consult your T1/E1 carrier. Click the drop-down menu button and select the line coding type:

B8ZS = Bipolar with 8-Zero Substitution. B8ZS is a bipolar line code that maintains an AC signal. If a long string of zeros occurs on a line, the signal approaches DC and loses synchronization. To synchronize the line, B8ZS replaces a string of 8 consecutive zeros with an 8-bit B8ZS code (actually called a bipolar violation) when transmitting a message. On the receiving end, the B8ZS code is removed. This is the default selection for T1, and it is not available for E1.

HDB3 = High Density Bipolar 3-Zero. HDB3 is a bipolar line code that also maintains an AC signal and line synchronization. It substitutes one of four bit patterns for every string of four consecutive zeros. The bit patterns depend on the polarity and number of the preceding ones. CCITT Recommendation G.703 governs HDB3 coding. This is the default selection for E1, and it is not available for T1.

AMI = Alternative Mark Inversion. AMI is a bipolar line code that transmits binary zero as zero volts and binary one as either positive or negative depending on the previous pulse (each pulse transmitted is opposite the one before it). *If you choose this type, you must also enable **Data Inversion** below.*

Line Framing

This parameter sets the format of data frames. The framing format of the T1/E1 line must match that of your T1/E1 carrier, otherwise you receive line framing errors. Click the drop-down menu button and select the frame format that the T1/E1 carrier specifies for the line.

T1 selections:

ESF = Extended Super Frame. Each ESF comprises 24 frames of 192 bits each, plus a 193rd bit for timing, etc. This option provides enhanced signaling, error checking, and synchronization and allows testing on the line when the line is in use. This is the default selection for T1.

SF/D4 = Super Frame or D4. Each SF comprises 12 frames of 192 bits each, plus a 193rd bit for timing, error checking, etc.

E1 selections:

E1/CRC4 = E1 16-Frame Multiframe with CRC-4 error detection. The frame structure is as below, plus timeslot 0 of each frame in the multiframe carries 4-bit CRC signatures for error detection. This is the default selection for E1.

E1 = E1 16-Frame Multiframe. The frame structure (a multiframe) consists of 16 frames. Each frame is 256 bits, or 32 8-bit timeslots.

Buildout

Line buildout is a conditioning factor that limits loss of signal strength on the line. Your T1/E1 carrier provides information on how to set this option. The length of the line and the transmit power across it determine the buildout value, which is measured in decibels (dB). Click the drop-down menu button and select the buildout value for the line:

-0.0 dB = This is the default selection.

-7.5 dB

-15.0 dB

Clock Source

This parameter defines the type of transmit timing source to be used. Click the drop-down menu button and select the clock source for this line:

Line = Source of transmit timing is the device on the other end of the T1/E1 connection. This is the default selection.

Internal = Source of transmit timing is internal.

Data Inversion

Check the box to apply data inversion, which inverts all signals coming into and out of the interface (i.e., it turns ones to zeroes and vice versa). The box is not checked by default. *You must enable data inversion if you use **AMI** line coding.* You may need to enable data inversion if you are experiencing errors on the T1/E1 line, especially when using **SF/D4** line framing. If you enable data inversion here, be sure the other side of the WAN connection is also using data inversion.

Loopback

Loopback testing is used to diagnose problems in the network: a device transmits a signal that passes through the network and returns to the device that sent it. This selection sets the WAN port to respond appropriately to the transmitted signal. Click the drop-down menu button and select the loopback mode and configuration for this WAN port:

None = This port is not in loopback mode (the default selection).

Line = Set line loopback mode, which means that the entire packet is used for loopback testing.

Payload = Set payload loopback mode, which means that only the data and not the framing bits are used for loopback testing. This selection applies only to ESF line framing.

Timeslots

Check the numbers for the DS0 (Digital Signal 0) timeslots to use for this WAN interface. All are checked by default. These timeslots can be in any order—contiguous or noncontiguous. Your T1/E1 carrier provides information on how to configure this parameter. For T1, there are 24 timeslots of 64 Kbps each, for a total of 1536 Kbps. For E1, there are 31 timeslots of 64 Kbps each, for a total of 1984 Kbps. The **Currently:** field shows the total for checked timeslots.

Click **Clear All** to clear all timeslots, or **Set All** to set all timeslots.

Figure 3-12: Configuration | Interfaces | WAN Card in Slot N | Port A B as T1 or E1 screen, PPP tab

PPP Multilink Parameters		
Attribute	Value	Description
Enable PPP Multilink	<input type="checkbox"/>	Check to enable PPP Multilink on this WAN card. All interfaces on this WAN card are then joined into one Multilink bundle. After modifying this parameter, you must verify the IP address for this interface.

Apply Cancel

PPP Multilink Parameters tab

This tab lets you configure a PPP Multilink connection on this WAN interface. PPP (Point-to-Point Protocol) provides communication between two points over a serial interface, in this case a synchronous line. PPP Multilink (MP) bundles both WAN ports together into one point-to-point connection to enhance bandwidth. MP fragments the datagram and assigns data packets to both ports, usually alternating them between the two; i.e., packet 1 to Port A, packet 2 to Port B, and so on, to balance the load between them. At the destination, MP reassembles the packets in the correct order. RFC 1990 describes PPP Multilink.

Enable PPP Multilink

To enable PPP Multilink (MP) on this interface, check this box. The box is not checked by default.

If you enable MP, the system automatically assigns the IP address on this port to the other port. Verify that the correct (same) IP address is on both ports. If you disable MP, verify that each port has the correct (different) IP address. To verify the IP address, see the **IP Parameters** tab.

Apply / Cancel

To apply your settings to this interface and include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | Interfaces** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Interfaces** screen.

End of Chapter



System Configuration

System configuration means configuring parameters for system-wide functions in the VPN Concentrator.

Configuration | System

This section of the Manager lets you configure parameters for VPN Concentrator system-wide functions.

- **Servers:** identifying servers for authentication, accounting, DNS, DHCP, and NTP.
- **Address Management:** assigning addresses to clients as a tunnel is established.
- **Tunneling Protocols:** configuring PPTP, L2TP, IPSec LAN-to-LAN connections, and IKE proposals.
- **IP Routing:** configuring static routes, default gateways, OSPF, global DHCP, and redundancy (VRRP).
- **Management Protocols:** configuring and enabling built-in servers for FTP, HTTP/HTTPS, TFTP, Telnet, SNMP, and SSL.
- **Events:** handling system events via logs, FTP backup, SNMP traps, syslog, SMTP, and email.
- **General:** identifying the system, and setting the time and date.

See the appropriate chapter in this manual or the online help for each section.

Figure 4-1: Configuration | System screen

Configuration | System Save Needed

This section of the VPN 3000 Concentrator Series Manager lets you configure system-wide parameters.

In the left frame, or in the list of links below, click the parameters you want to configure:

- [Servers](#) -- authentication, accounting, DNS, DHCP, and NTP.
- [Address Management](#) -- address assignment options and address pools.
- [Tunneling Protocols](#) -- PPTP, L2TP, IPSec LAN-to-LAN, and IPSec IKE proposals.
- [IP Routing](#) -- static routes, default gateways, OSPF, global DHCP, and redundancy (VRRP).
- [Management Protocols](#) -- FTP, HTTP/HTTPS, TFTP, Telnet, SNMP, and SSL.
- [Events](#) -- defaults, classes, trap destinations, syslog and SMTP servers, and email.
- [General](#) -- system name, contact, location, and time and date.

End of Chapter



Servers

Configuring servers means identifying them to the VPN 3000 Concentrator so it can communicate with them correctly. These servers provide user authentication and accounting functions, convert hostnames to IP addresses, assign client IP addresses, and synchronize the system with network time. The VPN Concentrator functions as a client of these servers.

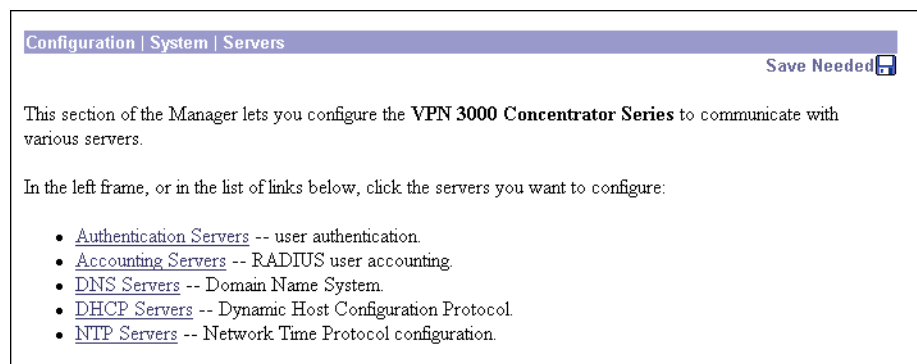
Configuration | System | Servers

This section of the Manager lets you configure the VPN Concentrator to communicate with servers for various functions.

- **Authentication Servers:** user authentication.
- **Accounting Servers:** RADIUS user accounting.
- **DNS Servers:** Domain Name System.
- **DHCP Servers:** Dynamic Host Configuration Protocol.
- **NTP Servers:** Network Time Protocol.

You can also configure the VPN Concentrator internal authentication server here if you have not already done so during Quick Configuration.

Figure 5-1: Configuration | System | Servers screen



Configuration | System | Servers | Authentication

This section lets you configure the VPN Concentrator internal server and external RADIUS, NT Domain, and SDI servers for authenticating users. To create and use a VPN, you must configure at least one authentication server type; i.e., at least one method of authenticating users.

If you check **Use Address from Authentication Server** on the **Configuration | System | Address Management | Assignment** screen, you must configure an authentication server here.

You must also configure servers here that correspond to the settings for **Authentication** method on the **IPSec Parameters** tab on the **Configuration | User Management | Base Group** and **Group** screens. For example, if you specify RADIUS authentication under IPSec for the base group, you must configure at least one RADIUS authentication server here. And in this example, the first RADIUS server is considered the primary server, the second RADIUS server is backup, etc.; any other server types are ignored.

Before you configure an external server here, be sure that the external server you reference is itself properly configured and that you know how to access it (IP address or hostname, TCP/UDP port, secret/password, etc.). The VPN Concentrator functions as the client of these servers.

The Cisco software CD-ROM includes a 30-day evaluation copy of Funk Software's Steel-Belted RADIUS authentication server and instructions for using it with the VPN Concentrator.

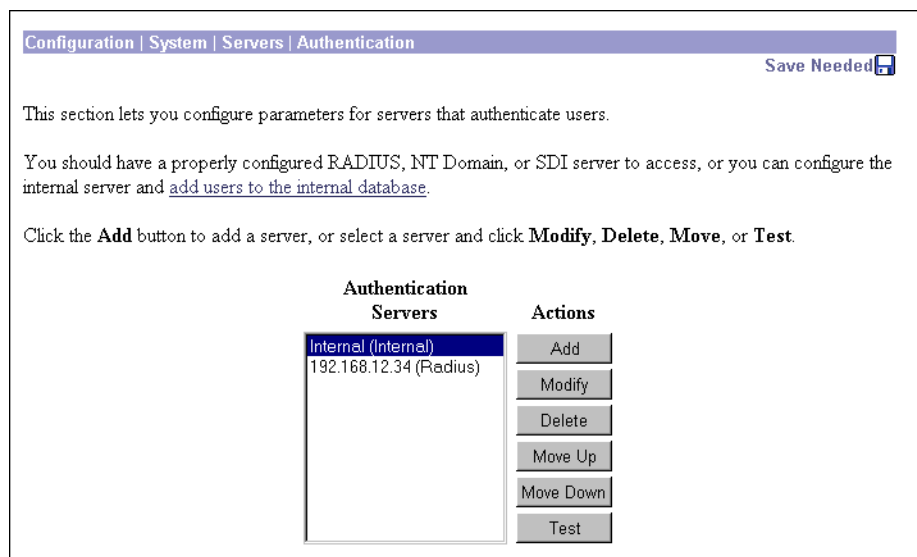
After you have configured an external authentication server, you can also test it. Testing sends a username and password to the server to determine that the VPN Concentrator is communicating properly with it, and that the server properly authenticates valid users and rejects invalid users.

If you configure the internal authentication server, you can add users to the internal database by clicking the highlighted link, which takes you to the **Configuration | User Management | Users** screen. To configure the internal server, you just add at least one user or group to the internal database.

If you configure **IPSec** on the **Quick Configuration | Protocols** screen, the VPN Concentrator automatically configures the internal authentication server. The internal server is also the default selection on the **Quick Configuration | Authentication** screen.

You can configure and prioritize up to 10 authentication servers here. The first server of a given type is the primary server for that type, and the rest are backup servers in case the primary is inoperative.

Figure 5-2: Configuration | System | Servers | Authentication screen



Authentication Servers

The **Authentication Servers** list shows the configured servers, in priority order. Each entry shows the server identifier and type; e.g., 192.168.12.34 (Radius). If no servers have been configured, the list shows **--Empty--**. The first server of each type is the primary, the rest are backup.

Add / Modify / Delete / Move / Test

To configure a new user authentication server, click **Add**. The Manager opens the **Configuration | System | Servers | Authentication | Add** screen.

To modify a configured user authentication server, select the server from the list and click **Modify**. The Manager opens the **Configuration | System | Servers | Authentication | Modify** screen. The internal server has no configurable parameters, therefore there is no **Modify** screen. If you select the internal server and click **Modify**, the Manager displays an error message.

To remove a configured user authentication server, select the server from the list and click **Delete**. *There is no confirmation or undo, except for the Internal Server (see the **Configuration | System | Servers | Authentication | Delete** screen).* The Manager refreshes the screen and shows the remaining entries in the **Authentication Servers** list.

Note: If you delete a server, users authenticated by that server will no longer be able to access the VPN unless another configured server can authenticate them.

To change the priority order for configured servers, select the entry from the list and click **Move** ↑ or **Move** ↓. The Manager refreshes the screen and shows the reordered **Authentication Servers** list.

To test a configured external user authentication server, select the server from the list and click **Test**. The Manager opens the **Configuration | System | Servers | Authentication | Test** screen. There is no need to test the internal server, and trying to do so returns an error message.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Servers | Authentication | Add or Modify

These screens let you:

Add: Configure and add a new user authentication server.

Modify: Modify parameters for a configured user authentication server.

Click the drop-down menu button and select the **Server Type**. The screen and its configurable fields change depending on the **Server Type**. Choices are:

RADIUS = An external Remote Authentication Dial-In User Service server (default).

NT Domain = An external Windows NT Domain server.

SDI = An external RSA Security Inc. SecurID server.

Internal Server = The internal VPN Concentrator authentication server. With this server, you can configure a maximum of 100 groups and users (combined) in the internal database. See **Configuration | User Management** for details.

Find your selected **Server Type** below.

Server Type = RADIUS

Configure these parameters for a RADIUS (Remote Authentication Dial-In User Service) authentication server.

Figure 5-3: Configuration | System | Servers | Authentication | Add or Modify RADIUS screen

The screenshot shows two overlapping windows from a configuration interface. The top window is titled 'Configuration | System | Servers | Authentication | Modify' and contains the text 'Change a configured user authentication server.' The bottom window is titled 'Configuration | System | Servers | Authentication | Add' and contains the following configuration options:

- Server Type:** A dropdown menu set to 'RADIUS'. A note next to it says: 'Selecting *Internal Server* will let you add users to the internal user database.'
- Authentication Server:** A text input field with the instruction 'Enter IP address or hostname.'
- Server Port:** A text input field with '0' entered and the instruction 'Enter 0 for default port (1645).'
- Timeout:** A text input field with '4' entered and the instruction 'Enter the timeout for this server (seconds).'
- Retries:** A text input field with '2' entered and the instruction 'Enter the number of retries for this server.'
- Server Secret:** A text input field with the instruction 'Enter the RADIUS server secret.'
- Verify:** A text input field with the instruction 'Re-enter the secret.'

At the bottom of the 'Add' window are two buttons: 'Add' and 'Cancel'.

Authentication Server

Enter the IP address or hostname of the RADIUS authentication server; e.g., 192.168.12.34. Maximum 32 characters. (If you have configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 1645.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. Minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next RADIUS authentication server in the list. Minimum is 0, default is 2, maximum is 10 retries.

Server Secret

Enter the RADIUS server secret (also called the shared secret); e.g., C8z077f. Maximum 64 characters. The field shows only asterisks.

Verify

Re-enter the RADIUS server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the **Configuration | System | Servers | Authentication** screen. Any new server appears at the bottom of the **Authentication Servers** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Authentication** screen, and the **Authentication Servers** list is unchanged.

Server Type = NT Domain

Configure these parameters for a Windows NT Domain authentication server.

Figure 5-4: Configuration | System | Servers | Authentication | Add or Modify NT Domain screen

Configuration | System | Servers | Authentication | Modify

Change a configured user authentication server.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Address Enter the IP address.

Server Port Enter 0 for default port (139).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Domain Controller Name Enter the NT Primary Domain Controller name for this authentication server.

Authentication Server Address

Enter the IP address of the NT Domain authentication server; e.g., 192.168.12.34. Use dotted decimal notation.

Server Port

Enter the TCP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 139.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. Minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next NT Domain authentication server in the list. Minimum is 0, default is 2, maximum is 10 retries.

Domain Controller Name

Enter the NT Primary Domain Controller hostname for this server; e.g., PDC01. Maximum 16 characters. You *must* enter this name, and it *must* be the correct hostname for the server whose IP address you entered in **Authentication Server Address** above; if it is incorrect, authentication will fail.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the **Configuration | System | Servers | Authentication** screen. Any new server appears at the bottom of the **Authentication Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Authentication** screen, and the **Authentication Servers** list is unchanged.

Server Type = SDI

Configure these parameters for an RSA Security Inc. SecurID authentication server.

Figure 5-5: Configuration | System | Servers | Authentication | Add or Modify SDI screen

Configuration | System | Servers | Authentication | Modify

Change a configured user authentication server.

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server Enter IP address or hostname.

Server Port Enter 0 for default port (5500).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Authentication Server

Enter the IP address or hostname of the SDI authentication server; e.g., 192.168.12.34. Maximum 32 characters. (If you have configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the server. Enter 0 (the default) to have the system supply the default port number, 5500.

Timeout

Enter the time in seconds to wait after sending a query to the server and receiving no response, before trying again. Minimum is 1 second, default is 4 seconds, maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the server after the timeout period. If there is still no response after this number of retries, the VPN Concentrator declares this server inoperative and uses the next SDI authentication server in the list. Minimum is 0, default is 2, maximum is 10 retries.

Add or Apply / Cancel

To add the new server to the list of configured user authentication servers, click **Add**. Or to apply your changes to the configured server, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the **Configuration | System | Servers | Authentication** screen. Any new server appears at the bottom of the **Authentication Servers** list.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Authentication** screen, and the **Authentication Servers** list is unchanged.

Server Type = Internal Server

The VPN Concentrator internal authentication server lets you enter a maximum of 100 groups and users (combined) in its database. To do so, see the **Configuration | User Management** screens, or click the highlighted link on the **Configuration | System | Servers | Authentication** screen.

The internal server has no configurable parameters, therefore there is no **Modify** screen. If you select the internal server and click **Modify** on the **Configuration | System | Servers | Authentication** screen, the Manager displays an error message.

You can configure only one instance of the internal server.

Figure 5-6: Configuration | System | Servers | Authentication | Add Internal Server screen

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Add / Cancel

To add the internal server to the list of configured user authentication servers, and to include the entry in the active configuration, click **Add**. The Manager returns to the **Configuration | System | Servers | Authentication** screen. The new server appears at the bottom of the **Authentication Servers** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Authentication** screen, and the **Authentication Servers** list is unchanged.


Configuration | System | Servers | Authentication | Delete

This screen asks you to confirm your decision to delete the internal authentication server. Deleting it prevents IPSec LAN-to-LAN connections, since they depend on internally configured groups for IPSec SA negotiations. Deleting it also prevents connections by all users that are configured in the internal user database.

*We strongly recommend that you **not** delete the internal authentication server.*

Figure 5-7: Configuration | System | Servers | Authentication | Delete screen

Configuration | System | Servers | Authentication | Delete

 You are about to delete the Internal Authentication Server. This will affect LAN-to-LAN configuration, and prevent users configured in the internal user database from connecting. Are you **sure** you want to delete it?

Delete the Internal Authentication Server

Do not delete the Internal Authentication Server

Yes / No

To delete the internal authentication server, click **Yes**. *There is no undo*. The Manager returns to the **Configuration | System | Servers | Authentication** screen and shows the remaining entries in the **Authentication Servers** list.

To not delete the internal authentication server, click **No**. The Manager returns to the **Configuration | System | Servers | Authentication** screen, and the **Authentication Servers** list is unchanged.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Servers | Authentication | Test

This screen let you test a configured external user authentication server to determine that:

- The VPN Concentrator is communicating properly with the authentication server.
- The server correctly authenticates a valid user.
- The server correctly rejects an invalid user.

Figure 5-8: Configuration | System | Servers | Authentication | Test screen

Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

User Name

Password

OK Cancel

User Name

To test connectivity and valid authentication, enter the username for a valid user who has been configured on the authentication server. Maximum 32 characters, case-sensitive.

To test connectivity and authentication *rejection*, enter a username that is *invalid* on the authentication server.

Password

Enter the password for the username above. Maximum 32 characters, case-sensitive. The field displays only asterisks.

OK / Cancel

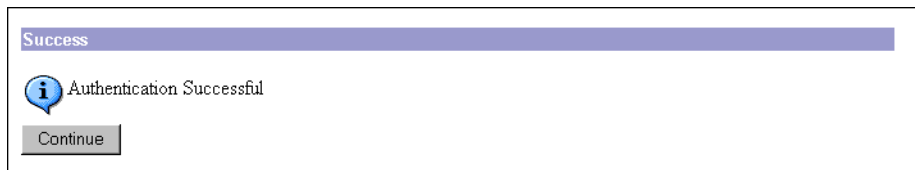
To send the username and password to the selected authentication server, click **OK**. The authentication and response process takes a few seconds. The Manager displays a **Success** or **Error** screen; see below.

To cancel the test and discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Authentication** screen.

Authentication Server Test: Success

If the VPN Concentrator communicates correctly with the authentication server, and the server correctly authenticates a valid user, the Manager displays a **Success** screen.

Figure 5-9: Authentication Server Test: Success screen



Continue

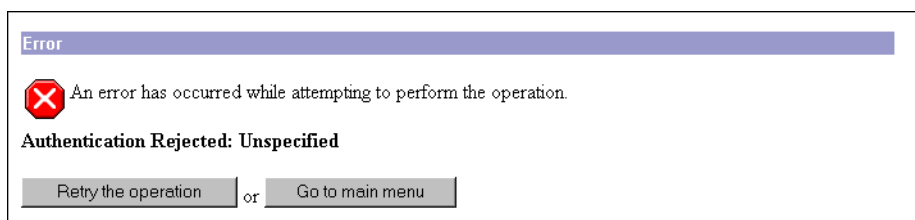
To return to the **Configuration | System | Servers | Authentication | Test** screen, click **Continue**. You can then test authentication for another username.

To return to the **Configuration | System | Servers | Authentication** screen, or any other screen, click the desired title in the left frame (Manager table of contents).

Authentication Server Test: Authentication Rejected Error

If the VPN Concentrator communicates correctly with the authentication server, *and the server correctly rejects an invalid user*, the Manager displays an **Authentication Rejected Error** screen.

Figure 5-10: Authentication Server Test: Authentication Rejected Error screen



To return to the **Configuration | System | Servers | Authentication | Test** screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

Authentication Server Test: Authentication Error

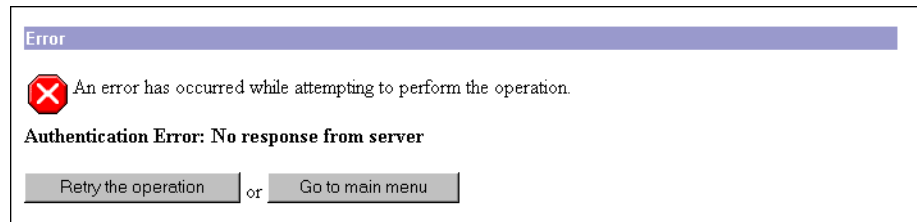
If the VPN Concentrator cannot communicate with the authentication server, the Manager displays an **Authentication Error** screen. Error messages include:

No response from server = There is no response from the selected server within the configured timeout and retry periods.

No active server found = The VPN Concentrator cannot find an active, configured server to test.

The server may be improperly configured or out of service, the network may be down or clogged, etc. Check the server configuration parameters, be sure the server is operating, check the network connections, etc.

Figure 5-11: Authentication Server Test: Authentication Error screen



To return to the **Configuration | System | Servers | Authentication | Test** screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

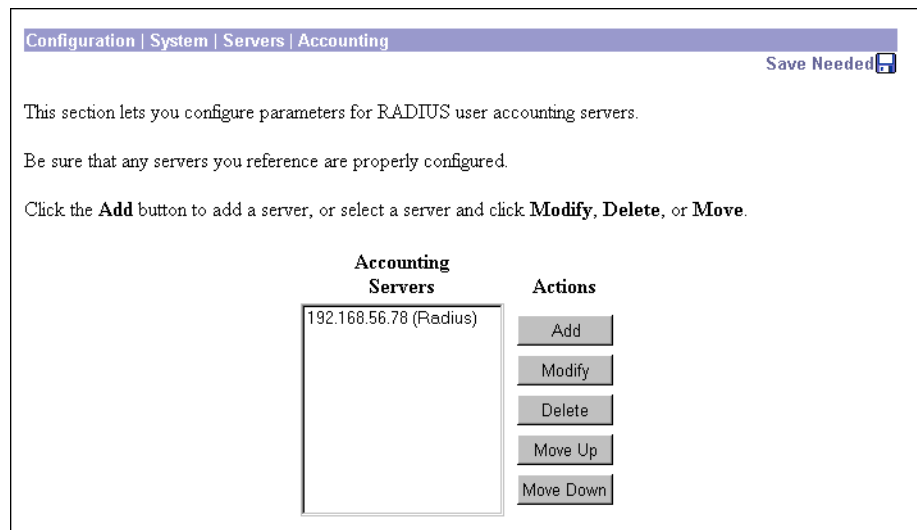
Configuration | System | Servers | Accounting

This section lets you configure external RADIUS user accounting servers, which collect data on user connect time, packets transmitted, etc., under the VPN tunneling protocols: PPTP, L2TP, and IPSec.

You can configure and prioritize up to 10 accounting servers. The first server is the primary, and the rest are backup servers in case the primary is inoperative.

Before you configure an accounting server here, be sure that the server you reference is itself properly configured and that you know how to access it (IP address or hostname, UDP port, server secret, etc.). The VPN Concentrator functions as the client of these servers.

Figure 5-12: Configuration | System | Servers | Accounting screen



The VPN Concentrator communicates with RADIUS accounting servers per RFC 2139 and currently includes the attributes in Table 5-1 in the accounting start and stop records. These attributes may change.

Table 5-1: RADIUS accounting record attributes

Start Record	Stop Record
User Name	User Name
Acct Status Type	Acct Status Type
Class	Class
Service Type	Service Type
Framed Protocol	Framed Protocol
Framed IP Address	Framed IP Address
NAS Port	NAS Port
Acct Session ID	Session Time
Tunnel Client Endpoint Address	Input Octets
Authentic	Output Octets
Delay Time	Input Packets
NAS IP Address	Output Packets
NAS Port Type	Terminate Cause
Tunnel Type	Acct Session ID
	Tunnel Client Endpoint Address
	Authentic
	Delay Time
	NAS IP Address
	NAS Port Type
	Tunnel Type

Accounting Servers

The **Accounting Servers** list shows the configured servers, in priority order. Each entry shows the server identifier and type; e.g., 192.168.12.34 (Radius). If no servers have been configured, the list shows --Empty--. The first server is the primary, the rest are backup.

Add / Modify / Delete / Move

To configure a new user accounting server, click **Add**. The Manager opens the **Configuration | System | Servers | Accounting | Add** screen.

To modify a configured user accounting server, select the server from the list and click **Modify**. The Manager opens the **Configuration | System | Servers | Accounting | Modify** screen.

To remove a configured user authentication server, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **Accounting Servers** list.

To change the priority order for configured servers, select the entry from the list and click **Move** ↑ or **Move** ↓. The Manager refreshes the screen and shows the reordered **Accounting Servers** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Servers | Accounting | Add or Modify

These screens let you:

Add: Configure and add a new RADIUS user accounting server.

Modify: Modify parameters for a configured RADIUS user accounting server.

Figure 5-13: Configuration | System | Servers | Accounting | Add or Modify screen

Configuration | System | Servers | Accounting | Add

Configure and add a RADIUS user accounting server.

Accounting Server Enter IP address or hostname.

Server Port Enter the server UDP port number.

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the server secret.

Accounting Server

Enter the IP address or hostname of the RADIUS accounting server; e.g., 192.168.12.34. (If you have configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the accounting server. The default is 1646.

Timeout

Enter the time in seconds to wait after sending a query to the accounting server and receiving no response, before trying again. Minimum is 1 second (the default), maximum is 30 seconds.

Retries

Enter the number of times to retry sending a query to the accounting server after the timeout period. If there is still no response after this number of retries, the system declares this server inoperative and uses the next accounting server in the list. Minimum is 0, default is 3, maximum is 10 retries.

Server Secret

Enter the server secret (also called the shared secret); e.g., C8z077f. The field shows only asterisks.

Verify

Re-enter the server secret to verify it. The field shows only asterisks.

Add or Apply / Cancel

To add this server to the list of configured user accounting servers, click **Add**. Or, to apply your changes to this user accounting server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Servers | Accounting** screen. Any new server appears at the bottom of the **Accounting Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | Accounting** screen, and the **Accounting Servers** list is unchanged.

Configuration | System | Servers | DNS

This screen lets you configure system-wide Domain Name System (DNS) servers. DNS servers convert domain names to IP addresses. Configuring DNS servers here lets you enter hostnames (e.g., mail01) rather than IP addresses as you configure and manage the VPN Concentrator.

You can configure up to three DNS servers that the system queries in order.

Figure 5-14: Configuration | System | Servers | DNS screen

Configuration | System | Servers | DNS

Configure system-wide DNS (Domain Name System) servers.

i Configuring DNS is optional, but it lets you use hostnames rather than IP addresses.

Enabled

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Timeout Period seconds

Timeout Retries

Apply Cancel

Enabled

To use DNS functions, check **Enabled** (the default). To disable DNS, clear the box.

Domain

Enter the name of the registered domain in which the VPN Concentrator is located; e.g., `altiga.com`. Maximum 48 characters. This entry is sometimes called the domain name suffix or sub-domain. The DNS system within the VPN Concentrator automatically appends this domain name to hostnames before sending them to a DNS server for resolution.

Primary DNS Server

Enter the IP address of the primary DNS server, using dotted decimal notation; e.g., `192.168.12.34`. Be sure this entry is correct to avoid DNS resolution delays.

Secondary DNS Server

Enter the IP address of the secondary (first backup) DNS server, using dotted decimal notation. If the primary DNS server doesn't respond to a query within the **Timeout Period** specified below, the system queries this server.

Tertiary DNS Server

Enter the IP address of the tertiary (second backup) DNS server, using dotted decimal notation. If the secondary DNS server doesn't respond to a query within the **Timeout Period** specified below, the system queries this server.

Timeout Period

Enter the initial time in seconds to wait for a response to a DNS query before sending the query to the next server. Minimum is 1, default is 2, maximum is 30 seconds. This time doubles with each retry cycle through the list of servers.

Timeout Retries

Enter the number of times to retry sending a DNS query to the configured servers, in order. In other words, this is the number of times to cycle through the list of servers before returning an error. Minimum is 0, default is 2, maximum is 10 retries.

Apply / Cancel

To apply your settings for DNS servers and include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Servers** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

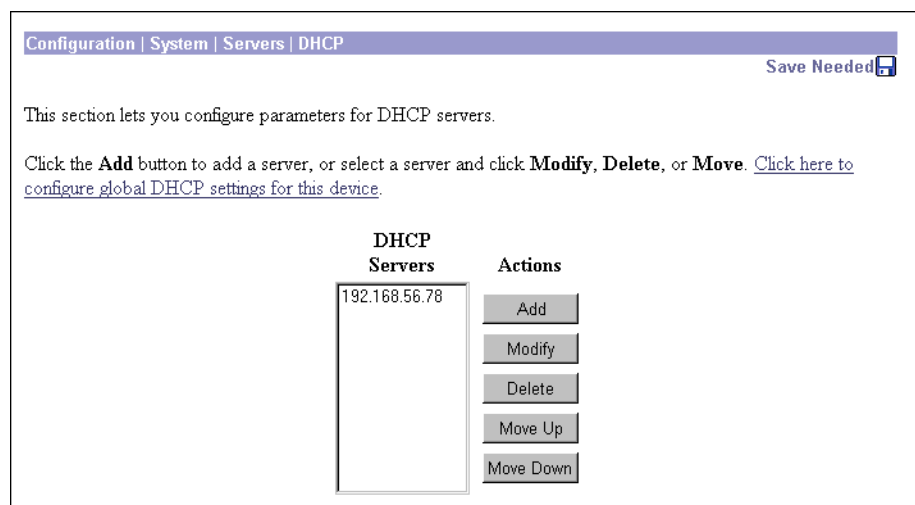
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Servers** screen.

Configuration | System | Servers | DHCP

This section of the Manager lets you configure Dynamic Host Configuration Protocol (DHCP) servers that assign IP addresses to clients as a VPN tunnel is established.

If you check **Use DHCP** on the **Configuration | System | Address Management | Assignment** screen, you must configure at least one DHCP server here. You should also configure global DHCP parameters on the **Configuration | System | IP Routing | DHCP** screen; click the highlighted link to go there. The DHCP system within the VPN Concentrator is enabled by default on that screen.

You can configure and prioritize up to three DHCP servers. The first server is the primary, and the rest are backup servers in case the primary is inoperative.

Figure 5-15: Configuration | System | Servers | DHCP screen

DHCP Servers

The **DHCP Servers** list shows the configured servers, in priority order. Each entry shows the server identifier, which can be an IP address or a hostname; e.g., 192.168.12.34. If no servers have been configured, the list shows **--Empty--**. The first server is the primary, the rest are backup.

Add / Modify / Delete / Move

To configure a new DHCP server, click **Add**. The Manager opens the **Configuration | System | Servers | DHCP | Add** screen.

To modify a configured DHCP server, select the server from the list and click **Modify**. The Manager opens the **Configuration | System | Servers | DHCP | Modify** screen.

To remove a configured DHCP server, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **DHCP Servers** list.

Note: If you delete a DHCP server, any IP addresses obtained from that server will eventually time out, and the associated sessions will terminate.

To change the priority order for configured servers, select the entry from the list and click **Move** ↑ or **Move** ↓. The Manager refreshes the screen and shows the reordered **DHCP Servers** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Servers | DHCP | Add or Modify

These screens let you:

Add: Configure and add a new DHCP server to the list of configured servers.

Modify: Modify the parameters for a configured DHCP server.

Figure 5-16: Configuration | System | Servers | DHCP | Add or Modify screen

DHCP Server

Enter the IP address or hostname of the DHCP server; e.g., 192 . 168 . 12 . 34. (If you have configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Server Port

Enter the UDP port number by which you access the DHCP server. The default is 67.

Add or Apply / Cancel

To add this server to the list of configured DHCP servers, click **Add**. Or, to apply your changes to this DHCP server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Servers | DHCP** screen. Any new server appears at the bottom of the **DHCP Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Servers | DHCP** screen, and the **DHCP Servers** list is unchanged.

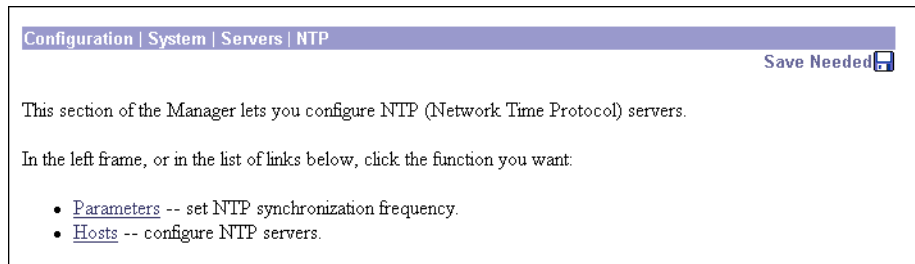
Configuration | System | Servers | NTP

This section of the Manager lets you configure NTP (Network Time Protocol) servers that the VPN Concentrator queries to synchronize with network time.

Clocks in many computers tend to drift a few seconds per day. Exact time synchronization is important for systems on a network so that protocol timestamps and events are accurate. Security certificates, for example, carry a timestamp that determines a time frame for their validity.

To make the NTP function operational, you must configure at least one NTP server (host). You can configure up to 10 NTP servers. The VPN Concentrator queries all of them and synchronizes its system clock with the derived network time.

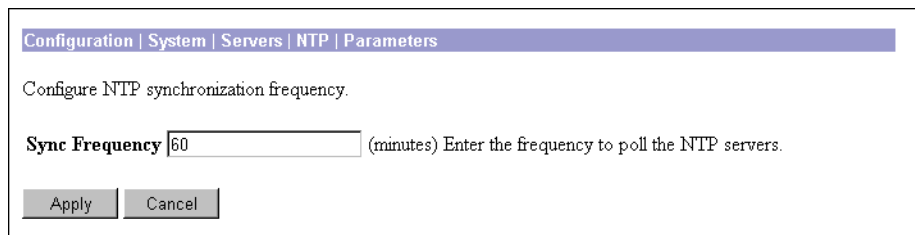
Figure 5-17: Configuration | System | Servers | NTP screen



Configuration | System | Servers | NTP | Parameters

This Manager screen lets you configure the NTP synchronization frequency parameter; i.e., how often the VPN Concentrator queries NTP servers to synchronize its clock with network time.

Figure 5-18: Configuration | System | Servers | NTP | Parameters screen



Sync Frequency

Enter the synchronization frequency in minutes. Minimum is 0, which disables the NTP function, default is 60, maximum is 10080 minutes (1 week).

Apply / Cancel

To apply your NTP parameter setting and include the setting in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Servers | NTP** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

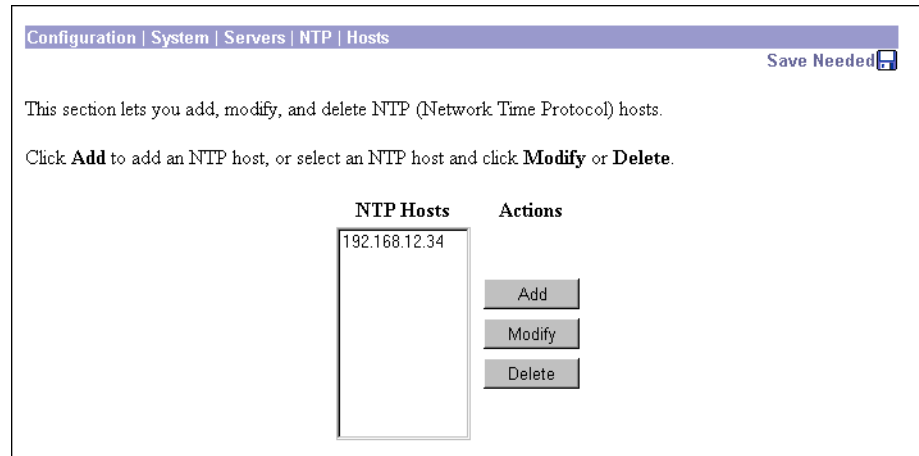
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Servers | NTP** screen.

Configuration | System | Servers | NTP | Hosts

This section of the Manager lets you add, modify, and delete NTP hosts (servers).

To make the NTP function operational, you must configure at least one NTP host. You can configure a maximum of 10 hosts. The VPN Concentrator queries all configured hosts and derives the correct network time from their responses.

Figure 5-19: Configuration | System | Servers | NTP | Hosts screen



NTP Hosts

The **NTP Hosts** list shows the configured servers. Each entry shows the server identifier, which can be an IP address or a hostname; e.g., 192.168.12.34. If no servers have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure a new NTP host (server), click **Add**. The Manager opens the **Configuration | System | Servers | NTP | Hosts | Add** screen.

To modify a configured NTP host, select the host from the list and click **Modify**. The Manager opens the **Configuration | System | Servers | NTP | Hosts | Modify** screen.

To remove a configured NTP host, select the host from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **NTP Hosts** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Servers | NTP | Hosts | Add or Modify

These screens let you:

Add a new NTP host to the list of configured hosts.

Modify a configured NTP host.

Figure 5-20: Configuration | System | Servers | NTP | Hosts | Add or Modify screen

NTP Host

Enter the IP address or hostname of the NTP host (server); e.g., 192.168.12.34. (If you have configured a DNS server, you can enter a hostname in this field; otherwise, enter an IP address.)

Add or Apply / Cancel

To add this host to the list of configured NTP hosts, click **Add**. Or, to apply your changes to a configured NTP host, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Servers | NTP | Hosts** screen. Any new host appears at the bottom of the **NTP Hosts** list.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entry, click **Cancel**. The Manager returns to the **Configuration | System | Servers | NTP | Hosts** screen, and the **NTP Hosts** list is unchanged.

End of Chapter



Address Management

IP addresses make internetworking connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number in order to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network; and once that connection is made, the second set connects client and server through the VPN tunnel.

In VPN Concentrator address management, we are dealing with the second set of IP addresses: those private IP addresses that connect a client with a resource on the private network, through the tunnel, and let the client function as if it were directly connected to the private network. Furthermore, we are dealing only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN Concentrator management.

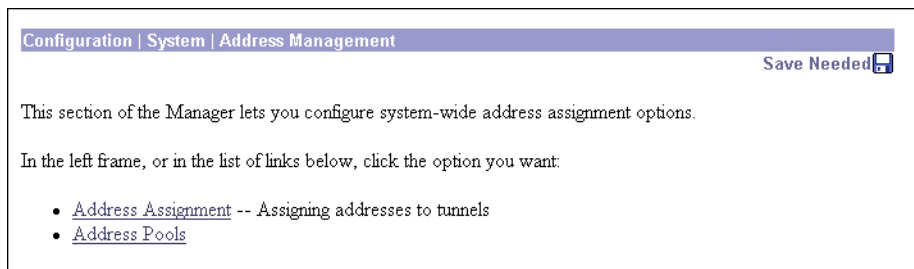
Therefore, when we discuss IP addresses here, we mean those IP addresses available in your private network addressing scheme, that let the client function as a tunnel endpoint.

Configuration | System | Address Management

This section of the VPN 3000 Concentrator Series Manager lets you configure options for assigning addresses to clients as a tunnel is established. A client must have an IP address to function as a tunnel endpoint.

- **Assignment** configures the prioritized methods for assigning IP addresses.
- **Pools** configures the internal address pools from which you can assign IP addresses.

Figure 6-1: Configuration | System | Address Management screen



Configuration | System | Address Management | Assignment

This screen lets you select prioritized methods for assigning IP addresses to clients as a tunnel is established. The VPN Concentrator tries the selected methods in the order listed until it finds a valid IP address to assign. You must select at least one method. You can select any and all methods. There are no default methods.

Figure 6-2: Configuration | System | Address Management | Assignment screen

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

- Use Client Address** Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server** Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP** Check to use DHCP to obtain an IP address for the client.
- Use Address Pools** Check to use internal address pool configuration to obtain an IP address for the client.

Apply Cancel

Use Client Address

Check this box to let the client specify its own IP address. For maximum security, we recommend that you control IP address assignment and *not use* client-specified IP addresses. Do not check *only* this box if you are using IPSec, since IPSec does not allow client-specified IP addresses.

Make sure the setting here is consistent with the setting for **Use Client Address** on the **PPTP/L2TP Parameters** tab on the **Configuration | User Management | Base Group** screen. A different **Use Client Address** setting for specific groups and users overrides the setting here and on the base group screen. See the **Configuration | User Management** screens.

Use Address from Authentication Server

Check this box to assign IP addresses retrieved from an authentication server on a per-user basis. If you are using an authentication server (external or internal) that has IP addresses configured, we recommend using this method.

Check this box if you enter an **IP Address** and **Subnet Mask** on the **Identity Parameters** tab on the **Configuration | User Management | Users | Add** or **Modify** screens (which means you are using the internal authentication server).

Use DHCP

Check this box to use a DHCP (Dynamic Host Configuration Protocol) server to assign IP addresses.

If you use DHCP, configure the server on the **Configuration | System | Servers | DHCP** and **Configuration | System | IP Routing | DHCP** screens.

Use Address Pools

Check this box to have the VPN Concentrator assign IP addresses from an internally configured pool.

If you use this method, configure the IP address pools on the **Configuration | System | Address Management | Pools** screens below.

Apply / Cancel

To include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | Address Management** screen.

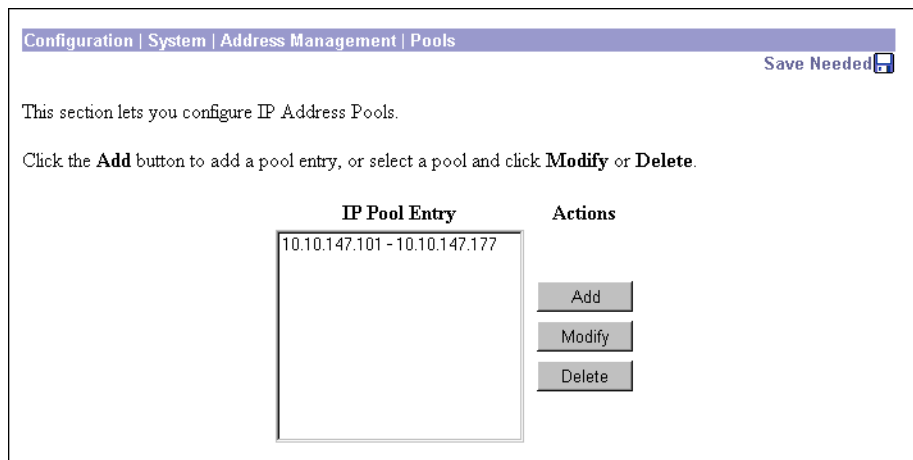
Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings or changes, click **Cancel**. The Manager returns to the **Configuration | Address Management** screen.

Configuration | System | Address Management | Pools

This section of the Manager lets you configure IP address pools from which the VPN Concentrator assigns addresses to clients. If you check **Use Address Pools** on the **Configuration | System | Address Management | Assignment** screen above, you must configure at least one address pool. The IP addresses in the pools must not be assigned to other network resources.

Figure 6-3: Configuration | System | Address Management | Pools screen



IP Pool Entry

The **IP Pool Entry** list shows each configured address pool as an address range; e.g., 10.10.147.100 - 10.10.147.177. If no pools have been configured, the list shows **--Empty--**. The pools are listed in the order they are configured. The system uses these pools in the order listed: if all addresses in the first pool have been assigned, it uses the next pool, and so on.

Add / Modify / Delete

To configure a new IP address pool, click **Add**. The Manager opens the **Configuration | System | Address Management | Pools | Add** screen.

To modify an IP address pool that has been configured, select the pool from the list and click **Modify**. The Manager opens the **Configuration | System | Address Management | Pools | Modify** screen.

To delete an IP address pool that has been configured, select the pool from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining pools in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Address Management | Pools | Add or Modify

These screens let you:

Add a new pool of IP addresses from which the VPN Concentrator assigns addresses to clients.

Modify an IP address pool that you have previously configured.

The IP addresses in the pool range must not be assigned to other network resources.

Figure 6-4: Configuration | System | Address Management | Pools | Add or Modify screen

Configuration | System | Address Management | Pools | Modify

Modify an address pool.

Configuration | System | Address Management | Pools | Add

Add an address pool.

Range Start Enter the start of the IP pool address range.

Range End Enter the end of the IP pool address range.

Add Cancel

Range Start

Enter the first IP address available in this pool. Use dotted decimal notation; e.g., 10.10.147.100.

Range End

Enter the last IP address available in this pool. Use dotted decimal notation; e.g., 10.10.147.177.

Add or Apply / Cancel

To add this IP address pool to the list of configured pools, click **Add**. Or to apply your changes to this IP address pool, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Address Management | Pools** screen. Any new pool appears at the end of the **IP Pool Entry** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Address Management | Pools** screen, and the **IP Pool Entry** list is unchanged.

End of Chapter



Tunneling Protocols

Tunneling protocols are the heart of virtual private networking. The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

The secure connection is called a tunnel, and the VPN 3000 Concentrator Series uses tunneling protocols to:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint or router.

The VPN Concentrator functions as a bidirectional tunnel endpoint: it can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination; or it can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

The VPN Concentrator supports the three most popular VPN tunneling protocols:

- PPTP: Point-to-Point Tunneling Protocol.
- L2TP: Layer 2 Tunneling Protocol.
- IPSec: IP Security Protocol.

It also supports L2TP over IPSec, which provides interoperability with the Windows 2000 VPN client and other remote-access clients that use that protocol.

This section explains how to configure the system-wide parameters for PPTP and L2TP, how to configure IPSec LAN-to-LAN connections, and how to configure IKE proposals for IPSec Security Associations and LAN-to-LAN connections.

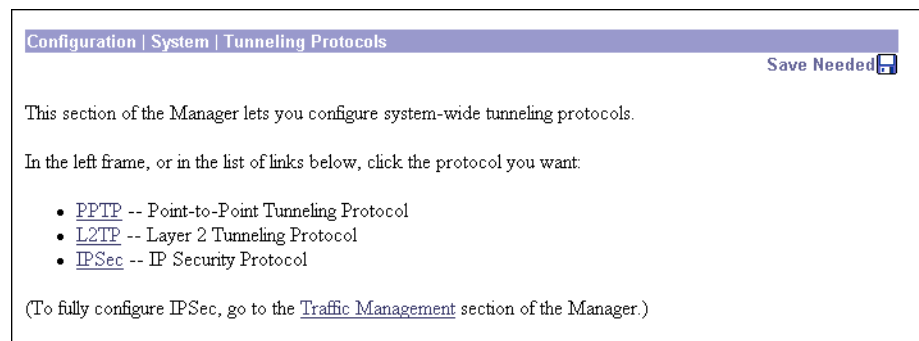
To configure L2TP over IPSec, see **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals**, and **Configuration | User Management**.

Configuration | System | Tunneling Protocols

This section of the Manager lets you configure system-wide parameters for tunneling protocols.

- **PPTP**: Configure PPTP parameters.
- **L2TP**: Configure L2TP parameters.
- **IPSec**: Configure IPSec parameters and connections.
 - **LAN-to-LAN**: IPSec LAN-to-LAN connections between two VPN Concentrators (or between the VPN Concentrator and another secure gateway).
 - **IKE Proposals**: IKE proposals for IPSec Security Associations and LAN-to-LAN connections.

Figure 7-1: Configuration | System | Tunneling Protocols screen



Configuration | System | Tunneling Protocols | PPTP

This screen lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) parameters.

The PPTP protocol defines mechanisms for establishing and controlling the tunnel, but uses Generic Routing Encapsulation (GRE) for data transfer.

PPTP is a client-server protocol. The VPN Concentrator always functions as a PPTP Network Server (PNS) and supports remote PC clients. The PPTP tunnel extends all the way from the PC to the VPN Concentrator.


PPTP is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000. PPTP is typically used with Microsoft encryption (MPPE).

You can configure PPTP on rules in filters; see **Configuration | Policy Management | Traffic Management**. Groups and users also have PPTP parameters; see **Configuration | User Management**.

Figure 7-2: Configuration | System | Tunneling Protocols | PPTP screen

Configuration | System | Tunneling Protocols | PPTP

This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.

 Disabling PPTP will terminate any active PPTP sessions.

Enabled

Maximum Tunnel Idle Time seconds

Packet Window Size packets

Limit Transmit to Window Check to limit the transmitted packets based on the peer's receive window.

Max. Tunnels Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel Enter 0 for unlimited sessions.

Packet Processing Delay 10^{ths} of seconds

Acknowledgement Delay milliseconds

Acknowledgement Timeout seconds

Note: Cisco supplies default settings for PPTP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the box to enable PPTP system-wide functions on the VPN Concentrator, or clear it to disable. The box is checked by default.

Caution: Disabling PPTP terminates any active PPTP sessions.

Maximum Tunnel Idle Time

Enter the time in seconds to wait before disconnecting an established PPTP tunnel with no active sessions. An open tunnel consumes system resources. Enter 0 to disconnect the tunnel immediately after the last session terminates (no idle time). Maximum is 86400 seconds (24 hours). The default is 5 seconds.

Packet Window Size

Enter the maximum number of received but unacknowledged PPTP packets that the system can buffer. The system must queue unacknowledged PPTP packets until it can process them. Minimum is 0, maximum is 32, default is 16 packets.

Limit Transmit to Window

Check the box to limit the number of transmitted PPTP packets to the client's packet window size. Ignoring the window improves performance, provided that the client can ignore the window violation. The box is not checked by default.

Max. Tunnels

Enter the maximum allowed number of simultaneously active PPTP tunnels. Minimum is 0, maximum depends on the VPN Concentrator model; e.g., Model 3060 = 5000. Enter 0 for unlimited tunnels (the default).

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per PPTP tunnel. Minimum is 0, maximum depends on the VPN Concentrator model; e.g., Model 3060 = 5000. Enter 0 for unlimited sessions (the default).

Packet Processing Delay

Enter the packet processing delay for PPTP flow control. This parameter is sent to the client in a PPTP control packet. Entries are in units of 100 milliseconds (0.1 second). Maximum is 65535; default is 1 (0.1 second).

Acknowledgement Delay

Enter the number of milliseconds that the VPN Concentrator will wait to send an acknowledgement to the client when there is no data packet on which to piggyback an acknowledgement. Enter 0 to send an immediate acknowledgement. Minimum delay is 50, maximum is 5000, default is 500 milliseconds.

Acknowledgement Timeout

Enter the number of seconds to wait before determining that an acknowledgement has been lost; i.e., before resuming transmission to the client even though the transmit window is closed. Minimum is 1, maximum is 10, default is 3 seconds.

Apply / Cancel

To apply your PPTP settings and to include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Configuration | System | Tunneling Protocols | L2TP

This screen lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) parameters.

L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding), and is regarded as a successor to both. The L2TP protocol defines mechanisms both for establishing and controlling the tunnel and for transferring data.


The VPN Concentrator always functions as a L2TP Network Server (LNS) and supports remote PC clients. The L2TP tunnel extends all the way from the PC to the VPN Concentrator. When the client PC is running Windows 2000, the L2TP tunnel is typically layered over an IPSec transport connection.

You can configure L2TP on rules in filters; see **Configuration | Policy Management | Traffic Management**. Groups and users also have L2TP parameters; see **Configuration | User Management**.

Figure 7-3: Configuration | System | Tunneling Protocols | L2TP screen

Configuration | System | Tunneling Protocols | L2TP

This section lets you configure system-wide L2TP (Layer 2 Tunneling Protocol) options.

 Disabling L2TP will terminate any active L2TP sessions.

Enabled

Maximum Tunnel Idle Time seconds

Control Window Size packets

Control Retransmit Interval seconds

Control Retransmit Limit Enter the maximum number of times to retransmit control packets.

Max. Tunnels Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel Enter 0 for unlimited sessions.

Hello Interval seconds

Note: Cisco supplies default settings for L2TP parameters that ensure optimum performance for typical VPN use. We strongly recommend that you not change the defaults without advice from Cisco personnel.

Enabled

Check the box to enable L2TP system-wide functions on the VPN Concentrator, or clear it to disable. The box is checked by default.

Caution: Disabling L2TP terminates any active L2TP sessions.

Maximum Tunnel Idle Time

Enter the time in seconds to wait before disconnecting an established L2TP tunnel with no active sessions. An open tunnel consumes system resources. Enter 0 to disconnect the tunnel immediately after the last session terminates (no idle time). Maximum is 86400 seconds (24 hours). The default is 60 seconds.

Control Window Size

Enter the maximum number of unacknowledged L2TP control channel packets that the system can receive and buffer. Minimum is 1, maximum is 16, and default is 4 packets.

Control Retransmit Interval

Enter the time in seconds to wait before retransmitting an unacknowledged L2TP tunnel control message to the remote client. Minimum is 1 (the default), and maximum is 10 seconds.

Control Retransmit Limit

Enter the number of times to retransmit L2TP tunnel control packets before assuming that the remote client is no longer responding. Minimum is 1, maximum is 32, and default is 4 times.

Max. Tunnels

Enter the maximum allowed number of simultaneously active L2TP tunnels. Minimum is 0, maximum depends on the VPN Concentrator model; e.g., Model 3060 = 5000. Enter 0 for unlimited tunnels (the default).

Max. Sessions/Tunnel

Enter the maximum number of sessions allowed per L2TP tunnel. Minimum is 0, maximum depends on the VPN Concentrator model; e.g., Model 3060 = 5000. Enter 0 for unlimited sessions (the default).

Hello Interval

Enter the time in seconds to wait when the L2TP tunnel is idle (no control or payload packets received) before sending a Hello (or “keep-alive”) packet to the remote client. Minimum is 1, maximum is 3600, and default is 60 seconds.

Apply / Cancel

To apply your L2TP settings and to include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols** screen.

Configuration | System | Tunneling Protocols | IPSec

This section of the Manager lets you configure IPSec LAN-to-LAN connections, and IKE (Internet Key Exchange) parameters for IPSec Security Associations and LAN-to-LAN connections.

IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN connections and client-to-LAN connections can use IPSec.

In IPSec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPSec, the two peers negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within the tunnel (the IPSec SA).

In IPSec LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In IPSec client-to-LAN connections, the VPN Concentrator functions only as responder. Initiators propose SAs; responders accept, reject, or make counter-proposals—all according to configured SA parameters. To establish a connection, both entities must agree on the SAs.

The Cisco VPN 3000 Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”).

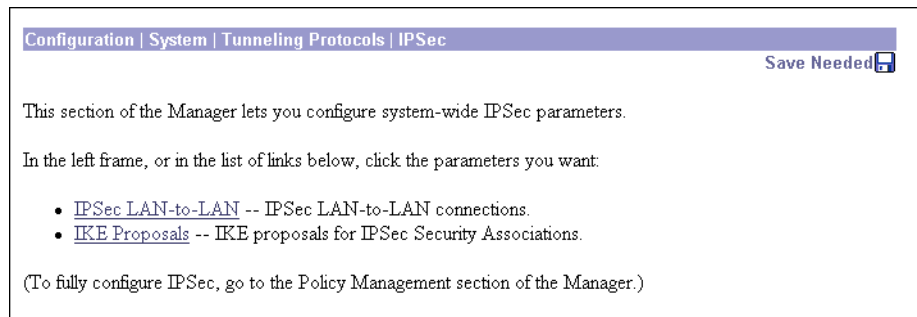
The Cisco VPN 3000 Client supports these IPSec attributes:

- Aggressive Negotiation Mode
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Group 1
- Encryption Algorithms:
 - DES-56
 - 3DES-168

- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode

You configure IKE proposals (parameters for the IKE SA) here. You apply them to IPSec LAN-to-LAN connections in this section, and to IPSec SAs on the **Configuration | Policy Management | Traffic Management | Security Associations** screens. Therefore, you should configure IKE proposals before configuring other IPSec parameters. Cisco supplies default IKE proposals that you can use or modify.

Figure 7-4: Configuration | System | Tunneling Protocols | IPSec screen



Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN

This section of the Manager lets you configure, add, modify, and delete IPSec LAN-to-LAN connections between two VPN Concentrators.

While the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN secure gateways, these instructions assume VPN Concentrators on both sides. And here, the “peer” is the other VPN Concentrator or secure gateway.

In a LAN-to-LAN connection, IPSec creates a tunnel between the public interfaces of two VPN Concentrators, which correspondingly route secure traffic to and from many hosts on their private LANs. There is no user configuration or authentication in a LAN-to-LAN connection; all hosts configured on the private networks can access hosts on the other side of the connection, at any time.

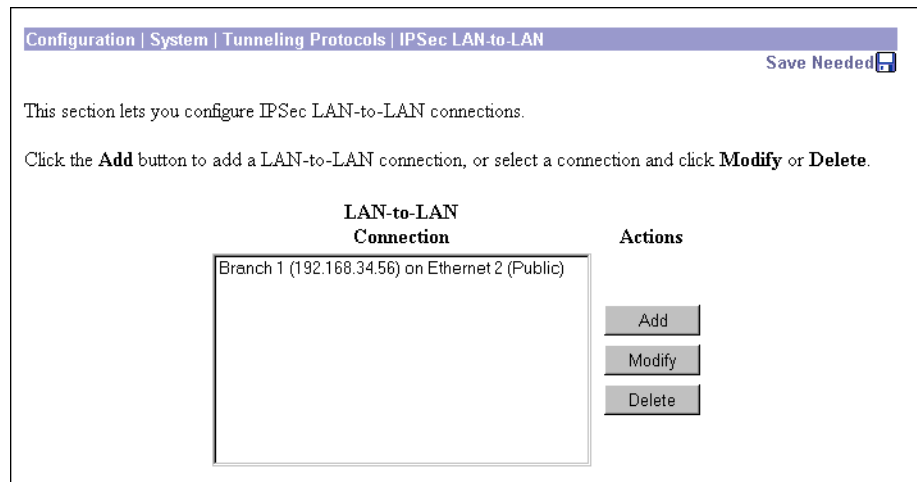
If you have a WAN connection as the public interface, you still use this section to configure a LAN-to-WAN connection.

To fully configure a LAN-to-LAN connection, you must configure identical basic IPSec parameters on both VPN Concentrators, and configure mirror-image private network addresses or network lists.

The VPN Concentrator also provides a network autodiscovery feature that dynamically discovers and updates the private network addresses on each side of the LAN-to-LAN connection, so you don’t have to explicitly configure them. This feature works only when both devices are VPN Concentrators. However, network autodiscovery is not allowed on a WAN interface.

You must configure a public interface on the VPN Concentrator before you can configure an IPSec LAN-to-LAN connection. See the **Configuration | Interfaces** screens. You must also configure IKE proposals before configuring LAN-to-LAN connections. See the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

Figure 7-5: Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN screen

LAN-to-LAN Connection

The **LAN-to-LAN Connection** list shows connections that have been configured. The connections are listed in the order you configure them, in the format: Name (Peer IP Address) on Interface; for example, Branch 1 (192.168.34.56) on Ethernet 2 (Public). If no connections have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new connection, click **Add**. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** screen. If you have not configured a public interface, the Manager displays the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | No Public Interfaces** screen.

To modify the parameters of a configured connection, select the connection from the list and click **Modify**. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify** screen.

To delete a configured connection, select the connection from the list and click **Delete**. *There is no confirmation or undo.* The Manager deletes the connection, its LAN-to-LAN filter rules, SAs, and group. The Manager then refreshes the screen and shows the remaining connections in the list.

Caution: Deleting a connection immediately deletes any tunnels—and user sessions—using that connection.

Reminder: *The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | No Public Interfaces

The Manager displays this screen if you have not configured a public interface on the VPN Concentrator and you try to add an IPsec LAN-to-LAN connection. The public interface need not be enabled, but it must be configured with an IP address and the **Public Interface** parameter enabled.

You should designate only one VPN Concentrator interface as a public interface.

Figure 7-6: Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | No Public Interfaces screen

Interface	Status	IP Address	Subnet Mask
Ethernet 2 (Public)	Not Configured		
WAN Interface in slot 2, port A	Not Configured		
WAN Interface in slot 2, port B	Not Configured		

Click the highlighted link to configure the desired public interface. The Manager opens the appropriate **Configuration | Interfaces** screen.

Configuration | System | Tunneling Protocols | IPsec LAN-to-LAN | Add or Modify

These screens let you:

Add: Configure and add a new IPsec LAN-to-LAN connection.

Modify: Modify parameters of a configured IPsec LAN-to-LAN connection.

You must configure a public interface on the VPN Concentrator before you can configure an IPsec LAN-to-LAN connection. See the **Configuration | Interfaces** screens.

You can configure only one LAN-to-LAN connection with each VPN Concentrator (or other secure gateway) peer.

Figure 7-7: Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify screen

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add

Add a new IPSec LAN-to-LAN connection.

Name	<input type="text"/>	Enter the name for this LAN-to-LAN connection.
Interface	<input type="text" value="Ethernet 2 (Public) (192.168.12.34)"/>	Select the interface to put this LAN-to-LAN connection on.
Peer	<input type="text"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Preshared Key	<input type="text"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication	<input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
Encryption	<input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery	<input type="checkbox"/>	Check to automatically discover networks. Parameters below are ignored if checked.

Local Network

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	

Remote Network

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text"/>	

When you **Add** or **Modify** a connection on these screens, the VPN Concentrator automatically:

- Creates or modifies two filter rules with the **Apply IPSec** action: one inbound, one outbound, named L2L:<Name> In and L2L:<Name> Out.
- Creates or modifies an IPSec Security Association named L2L:<Name>.
- Applies these rules to the filter on the public interface and applies the SA to the rules. If the public interface doesn't have a filter, it applies the Public (default) filter with the rules above.
- Creates or modifies a group named with the **Peer** IP address. If the VPN Concentrator internal authentication server hasn't been configured, it does so, and adds the group to the database.

All of the rules, SAs, filters, and group have default parameters or those specified on this screen. You can modify the rules and SA on the **Configuration | Policy Management | Traffic Management** screens, the group on the **Configuration | User Management | Groups** screens, and the interface on the **Configuration | Interfaces** screens. However, we recommend that you keep the configured defaults. You cannot delete these rules, SAs, or group individually; the system automatically deletes them when you delete the LAN-to-LAN connection.

To fully configure a LAN-to-LAN connection, you must configure identical IPSec LAN-to-LAN parameters on both VPN Concentrators, and configure mirror-image local and remote private network addresses. For example:

Configure	On this VPN Concentrator	On peer VPN Concentrator
Local Network	10.10.0.0/0.0.255.255	11.0.0.0/0.255.255.255
Remote Network	11.0.0.0/0.255.255.255	10.10.0.0/0.0.255.255

If you use network lists, you must also configure and apply them as mirror images on the two VPN Concentrators. If you use network autodiscovery, you must use it on both VPN Concentrators.

Caution: On the **Modify** screen, any changes take effect as soon as you click **Apply**. If client sessions are using this connection, changes delete the tunnel—and the sessions—without warning.

Name

Enter a unique descriptive name for this connection. Maximum 32 characters. Since the created rules and SA use this name, we recommend that you keep it short.

Interface

Add screen:

Click the drop-down menu button and select the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. The list shows all interfaces (Ethernet or WAN) that have the **Public Interface** parameter enabled. See **Configuration | Interfaces**.

Modify screen:

The screen shows the configured public interface on this VPN Concentrator for this end of the LAN-to-LAN connection. You cannot change the interface. To move the connection to another interface, you must delete this connection and add a new one for the other interface.

Peer

Enter the IP address of the remote peer in the LAN-to-LAN connection. This must be the IP address of the public interface on the peer VPN Concentrator. Use dotted decimal notation; e.g., 192.168.34.56.

Digital Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under **Administration | Certificate Management**.

Click the drop-down menu button and select the option. The list shows any digital certificates that have been installed, plus:

None (Use Preshared Keys) = Use only preshared keys to authenticate the peer during Phase 1 IKE negotiations. This is the default selection.

Preshared Key

Enter a preshared key for this connection. Use a minimum of 4, a maximum of 32 alphanumeric characters; e.g, sZ9s14ep7. The system displays your entry in clear text. Even if you use a PKI digital certificate, enter a key in this field.

This key becomes the password for the IPsec LAN-to-LAN group that is created, and you must enter the same key on the peer VPN Concentrator. (This is *not* a manual encryption or authentication key. The system automatically generates those session keys.)

Authentication

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity” in VPN literature. The IPsec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication.

Click the drop-down menu button and select the algorithm:

None = No data authentication.

ESP/MD5/HMAC-128 = ESP protocol using HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.

ESP/SHA/HMAC-160 = ESP protocol using HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the drop-down menu button and select the algorithm:

Null = Use ESP without encryption; no packet encryption.

DES-56 = Use DES encryption with a 56-bit key.

3DES-168 = Use Triple-DES encryption with a 168-bit key. This selection is the most secure and it is the default selection.

IKE Proposal

This parameter specifies the set of attributes for Phase 1 IPSec negotiations, which are known as IKE proposals. See the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. You must configure, activate, and prioritize IKE proposals before configuring LAN-to-LAN connections.

Click the drop-down menu button and select the IKE proposal. The list shows only active IKE proposals in priority order. Cisco-supplied default active proposals are:

IKE-3DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys. This selection is the most secure, and it is the default selection.

IKE-3DES-MD5-DH1 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 1 to generate SA keys.

IKE-DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use DES-56 encryption. Use D-H Group 1 to generate SA keys.

Network Autodiscovery

Check this box to use the VPN Concentrator network autodiscovery feature that dynamically discovers and continuously updates the private network addresses on each side of the LAN-to-LAN connection. This feature uses RIP, and **Inbound RIP RIPv2/v1** must be enabled on the Ethernet 1 (Private) interface of both VPN Concentrators. See **Configuration | Interfaces**. If you check this box, skip the **Local** and **Remote Network** parameters below; they are ignored.

Network autodiscovery is not allowed on a WAN interface.

Local Network

These entries identify the private network—*on this VPN Concentrator*—whose hosts can use the LAN-to-LAN connection. These entries must match those in the **Remote Network** section on the peer VPN Concentrator.

Network List

Click the drop-down menu button and select the configured network list that specifies the local network addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

Use IP Address/Wildcard-mask below, which lets you enter a network address.

Create new Network List (on **Add** screen only), which lets you create a network list of local network addresses. The Manager automatically opens the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List** screen when you click **Add**; see description below.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard Mask** fields.

Note: An IP address is used with a *wildcard mask* to provide the desired granularity. A *wildcard mask* is the reverse of a subnet mask; i.e., the wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example:

0.0.0.0/255.255.255.255 = any address

10.10.1.35/0.0.0.0 = only 10.10.1.35

10.10.1.35/0.0.0.255 = all 10.10.1.nnn addresses

IP Address

Enter the IP address of the private local network on this VPN Concentrator. Use dotted decimal notation; e.g., 10.10.0.0.

Wildcard Mask

Enter the wildcard mask for the private local network. Use dotted decimal notation; e.g., 0.0.255.255. The system supplies a default wildcard mask appropriate to the IP address class.

Remote Network

These entries identify the private network—*on the remote peer VPN Concentrator*—whose hosts can use the LAN-to-LAN connection. These entries must match those in the **Local Network** section on the peer VPN Concentrator.

Network List

Click the drop-down menu button and select the configured network list that specifies the remote network addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

Use IP Address/Wildcard-mask below, which lets you enter a network address.

Create new Network List (on **Add** screen only), which lets you create a network list of remote network addresses. The Manager automatically opens the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Remote Network List** screen when you click **Add**; see description below.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard-mask** fields.

See the *wildcard mask* note above.

IP Address

Enter the IP address of the private network on the remote peer VPN Concentrator. Use dotted decimal notation; e.g. 11.0.0.0.

Wildcard Mask

Enter the wildcard mask for the private remote network. Use dotted decimal notation; e.g., 0.255.255.255. The system supplies a default wildcard mask appropriate to the IP address class.

Add or Apply / Cancel

Add screen: To add this connection to the list of configured LAN-to-LAN connections, click **Add**. If you are creating new network lists, the Manager automatically displays the appropriate **Local** or **Remote Network List** screens. Otherwise, the Manager displays the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Modify screen: To apply your changes to this LAN-to-LAN connection, click **Apply**. *Any changes take effect as soon as you click **Apply**. If client sessions are using this connection, changes delete the tunnel—and the sessions—without warning.* The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen, and the **LAN-to-LAN Connection** list is unchanged.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local or Remote Network List

These screens let you configure and add network lists for the **Local Network** or **Remote Network** of a new IPSec LAN-to-LAN connection. The Manager automatically opens these screens if you select **Create new Network List** under **Network List** on the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** screen.

A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens also.

On the **Local Network List** screen, the Manager can automatically generate a network list using the valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See **Monitoring | Routing Table**.)

A single network list can contain a maximum of 200 network entries.

Figure 7-8: Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local or Remote Network List screen

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Remote Network List

Configure and add a new Network List for the Remote end of an IPSec LAN-to-LAN connection.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Local Network List

Configure and add a new Network List for the Local end of an IPSec LAN-to-LAN connection. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/w.w.w.w** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

List Name

The Manager supplies a default name that identifies the list as a LAN-to-LAN local or remote list, which we recommend you keep. Otherwise, enter a unique name for this network list. Maximum 48 characters, case-sensitive. Spaces are allowed.

If you use the **Generate Local List** feature on the **Local Network List** screen, edit this name *after* the system generates the network list.

Network List

Enter the networks in this network list. Enter each network on a single line using the format `n.n.n.n/w.w.w.w`, where `n.n.n.n` is a network IP address and `w.w.w.w` is a wildcard mask.

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

If you omit the wildcard mask, the Manager supplies the default wildcard mask for the class of the network address. For example, 192.168.12.0 is a Class C address, and default wildcard mask is 0.0.0.255.

You can enter a maximum of 200 networks in a single network list.

Generate Local List

On the **Local Network List** screen, click this button to have the Manager automatically generate a network list using the first 200 valid network routes in the routing table for the Ethernet 1 (Private) interface of this VPN Concentrator. (See **Monitoring | Routing Table**.) The Manager refreshes the screen after it generates the list, and you can then edit the **Network List** and the **List Name**.

Note: The generated list replaces any existing entries in the **Network List**.

Add

To add this network list to the configured network lists, click **Add**. The Manager displays either the **Remote Network List** screen or the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done

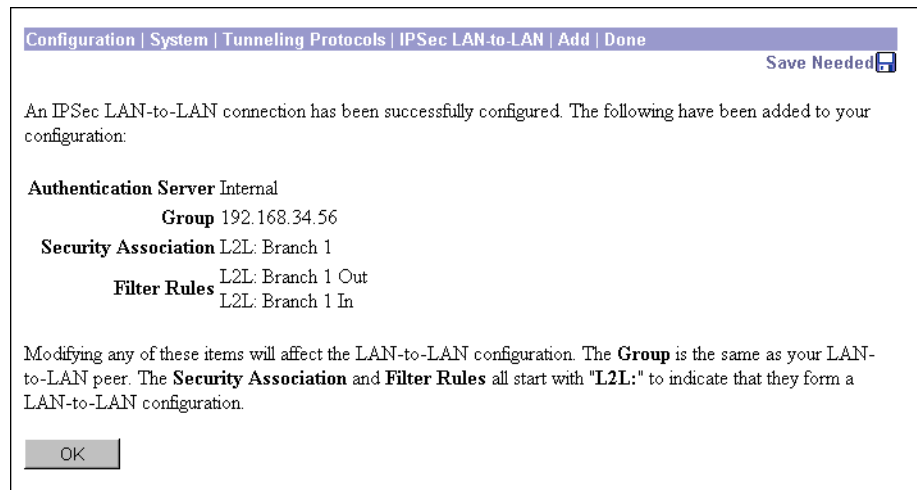
The Manager displays this screen when you have finished configuring all parameters for a new IPSec LAN-to-LAN connection. It documents the added configuration entities.

The Manager displays this screen only once. We suggest you print a copy of the screen to save it for your records.

To examine or modify an entity, see the appropriate screen:

- **Group:** See **Configuration | User Management | Groups**.
- **Security Association:** See **Configuration | Policy Management | Traffic Management | Security Associations**.
- **Filter Rules:** See **Configuration | Policy Management | Traffic Management | Rules**.

You cannot delete the group, SA, or rules individually, nor can you remove the rules from their filter. The system automatically deletes them when you delete the LAN-to-LAN connection.

Figure 7-9: Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done screen

OK

To close this screen and return to the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screen, click **OK**. The **LAN-to-LAN Connection** list shows the new connection, and the Manager includes all the new settings in the active configuration.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals

This section of the Manager lets you configure, add, modify, activate, deactivate, delete, and prioritize IKE proposals, which are sets of parameters for Phase 1 IPSec negotiations. During Phase 1, the two peers establish a secure tunnel within which they then negotiate the Phase 2 parameters.

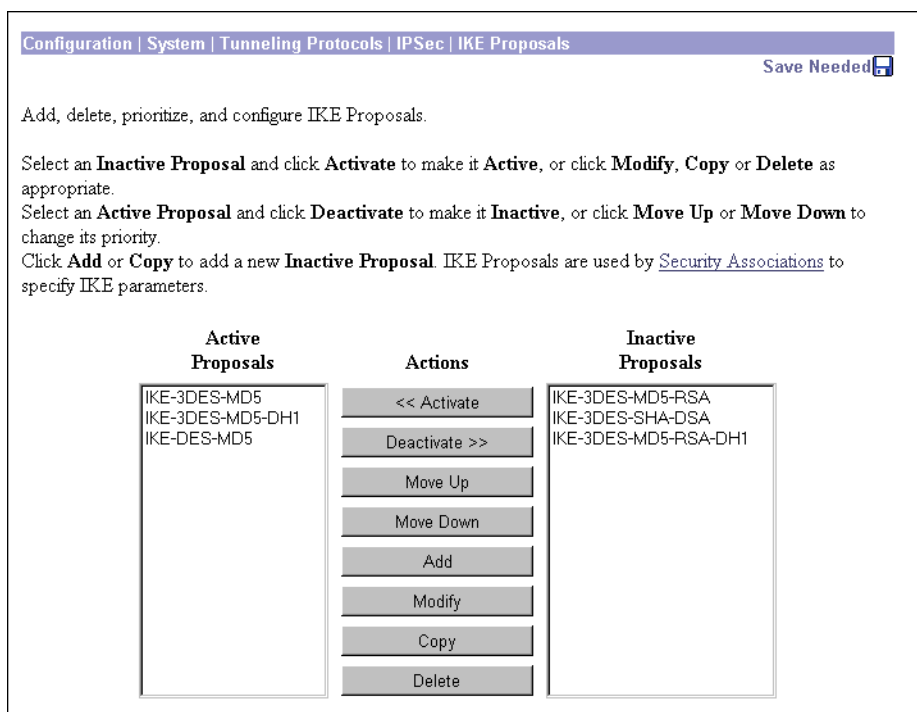
The VPN Concentrator uses IKE proposals both as initiator and responder in IPSec negotiations. In LAN-to-LAN connections, the VPN Concentrator can function as initiator or responder. In client-to-LAN connections, the VPN Concentrator functions only as responder.

You must configure, activate, and prioritize IKE proposals before you configure IPSec Security Associations. See **Configuration | Policy Management | Traffic Management | Security Associations**, or click the *Security Associations* link on this screen.

You must also configure and activate IKE proposals before configuring IPSec LAN-to-LAN connections. See **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** above.

You can configure a maximum of 25 IKE proposals total (active and inactive).

Figure 7-10: Configuration | System | Tunneling Protocols | IPSec | IKE Proposals screen



Cisco supplies default IKE proposals that you can use or modify; see Table 7-1. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add** for explanations of the parameters.

Table 7-1: Cisco-supplied default IKE Proposals

Proposal Name	IKE-3DES-MD5	IKE-3DES-MD5-DH1	IKE-DES-MD5	IKE-3DES-MD5-RSA	IKE-3DES-SHA-DSA	IKE-3DES-MD5-RSA-DH1
Parameter	Active by default	Active by default	Active by default	Inactive by default	Inactive by default	Inactive by default
Authentication Mode	Preshared Keys	Preshared Keys	Preshared Keys	RSA Digital Certificate	DSA Digital Certificate	RSA Digital Certificate
Authentication Algorithm	MD5/HMAC-128	MD5/HMAC-128	MD5/HMAC-128	MD5/HMAC-128	SHA/HMAC-160	MD5/HMAC-128
Encryption Algorithm	3DES-168	3DES-168	DES-56	3DES-168	3DES-168	3DES-168
Diffie-Hellman Group	Group 2 (1024-bits)	Group 1 (768-bits)	Group 1 (768-bits)	Group 2 (1024-bits)	Group 2 (1024-bits)	Group 1 (768-bits)
Lifetime Measurement	Time	Time	Time	Time	Time	Time
Data Lifetime	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)
Time Lifetime	86400 sec	86400 sec	86400 sec	86400 sec	86400 sec	86400 sec

Active Proposals

The field shows the names of IKE proposals that have been configured, activated, and prioritized. As an IPSec responder, the VPN Concentrator checks these proposals in priority order, to see if it can find one that agrees with parameters in the initiator's proposed SA.

Activating a proposal also makes it available for use wherever the Manager displays an **IKE Proposal** list, and the first active proposal appears as the default selection.

Inactive Proposals

The field shows the names of IKE proposals that have been configured but are inactive. New proposals appear in this list when you first configure and add them. The VPN Concentrator does not use these proposals in any IPSec negotiations, nor do they appear in **IKE Proposal** lists.

Note: To configure L2TP over IPSec, you must activate **IKE-3DES-MD5-RSA**. Also see the **Configuration | User Management** screens.

<< Activate

To activate an inactive IKE proposal, select it from the **Inactive Proposals** list and click this button. The Manager moves the proposal to the **Active Proposals** list and refreshes the screen.

>> Deactivate

To deactivate an active IKE proposal, select it from the **Active Proposals** list and click this button. If the active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can deactivate it. Otherwise, the Manager moves the proposal to the **Inactive Proposals** list and refreshes the screen.

Move Up / Move Down

To change the priority order of an active IKE proposal, select it from the **Active Proposals** list and click **Move Up** or **Move Down**. The Manager refreshes the screen and shows the reordered **Active Proposals** list. These actions move the proposal up or down one position.

Add

To configure and add a new IKE proposal to the list of **Inactive Proposals**, click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add**.

Modify

To modify a configured IKE proposal, select it from either **Active Proposals** or **Inactive Proposals** and click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify**. Modifying an active proposal does not affect connections currently using it, but changes do affect subsequent connections.

Copy

To use a configured IKE proposal as the basis for configuring and adding a new one, select it from either **Active Proposals** or **Inactive Proposals** and click this button. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy**. The new proposal appears in the **Inactive Proposals** list.

Delete

To delete a configured IKE proposal, select it from either **Active Proposals** or **Inactive Proposals** and click this button. If an active proposal is configured on a Security Association, the Manager displays an error message; and you must remove it from the SA before you can delete it. *Otherwise, there is no confirmation or undo.* The Manager refreshes the screen and shows the remaining IKE proposals in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy

These screens let you:

Add: Configure and add a new inactive IKE proposal.

Modify: Modify a previously configured IKE proposal.

Copy: Copy a configured IKE proposal, modify its parameters, save it with a new name, and add it to the configured inactive IKE proposals.

You can configure a maximum of 25 IKE proposals total (active and inactive).

Figure 7-11: Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy screen

The screenshot shows three overlapping windows for configuring IKE proposals:

- Top Window (Copy):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Copy. Text: Copy a configured IKE Proposal.
- Middle Window (Modify):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify. Text: Modify a configured IKE Proposal.
- Bottom Window (Add):** Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add. Text: Configure and add a new IKE Proposal.

The 'Add' window contains the following fields and options:

Proposal Name	<input type="text"/>	Specify the name of this IKE Proposal.
Authentication Mode	Preshared Keys	Select the authentication mode to use.
Authentication Algorithm	MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 2 (1024-bits)	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.

Buttons: Add, Cancel

Proposal Name

Enter a unique name for this IKE proposal. Maximum is 48 characters, case-sensitive. Spaces are allowed.

Authentication Mode

This parameter specifies how to authenticate the remote client or peer. Authentication proves that the connecting entity is who you think it is. If you select one of the digital certificate modes, an appropriate digital certificate must be installed on this VPN Concentrator and the remote client or peer. See the discussion under **Administration | Certificate Management**.

Click the drop-down menu button and select the method:

Preshared Keys = Use preshared keys (the default). The keys are derived from the password of the user's or peer's group.

RSA Digital Certificate = Use a digital certificate with keys generated by the RSA algorithm.

DSA Digital Certificate = Use a digital certificate with keys generated by the DSA algorithm.

Authentication Algorithm

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from.

Click the drop-down menu button and select the algorithm:

MD5/HMAC-128 = HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.

SHA/HMAC-160 = HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption Algorithm

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the drop-down menu button and select the algorithm:

DES-56 = DES encryption with a 56-bit key.

3DES-168 = Triple-DES encryption with a 168-bit key. This is the default selection, and it is the most secure.

Diffie-Hellman Group

This parameter specifies the Diffie-Hellman group used to generate IPsec SA keys. The Diffie-Hellman technique generates keys using prime numbers and “generator” numbers in a mathematical relationship.

Click the drop-down menu button and select the group:

Group 1 (768-bits) = Use Diffie-Hellman Group 1 to generate IPsec SA keys, where the prime and generator numbers are 768 bits. Select this option if you select **DES-56** under **Encryption Algorithm** above.

Group 2 (1024-bits) = use Diffie-Hellman Group 2 to generate IPsec SA keys, where the prime and generator numbers are 1024 bits. This is the default selection for use with the **3DES-168 Encryption Algorithm** above, and it is the most secure.

Lifetime Measurement

This parameter specifies how to measure the lifetime of the IKE SA keys, which is how long the IKE SA lasts until it expires and must be renegotiated with new keys. It is used with the **Data Lifetime** or **Time Lifetime** parameters below.

Click the drop-down menu button and select the measurement method:

Time = Use time (seconds) to measure the lifetime of the SA (the default). Configure the **Time Lifetime** parameter below.

Data = Use data (number of kilobytes) to measure the lifetime of the SA. Configure the **Data Lifetime** parameter below.

Both = Use both time and data, whichever occurs first, to measure the lifetime. Configure both **Time Lifetime** and **Data Lifetime** parameters.

None = No lifetime measurement. The SA lasts until the connection is terminated for other reasons.

Data Lifetime

If you select **Data** or **Both** under **Lifetime Measurement** above, enter the number of kilobytes of payload data after which the IKE SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.

Time Lifetime

If you select **Time** or **Both** under **Lifetime Measurement** above, enter the number of seconds after which the IKE SA expires. Minimum is 60 seconds, default is 86400 seconds (24 hours), maximum is 2147483647 seconds (about 68 years).

Add or Apply / Cancel

Add or **Copy** screen:

To add this IKE proposal to the list of **Inactive Proposals**, click **Add** or **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. To use the new proposal, you must activate and prioritize it as explained for that screen.

Modify screen:

To apply your changes to this IKE proposal, click **Apply**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. If you modify an active proposal, changes do not affect connections currently using it, but they do affect subsequent connections.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen, and the IKE proposals lists are unchanged.

End of Chapter



IP Routing

In a typical installation, the VPN Concentrator is connected to the public network through an external router, which routes data traffic between networks, and it may also be connected to the private network through a router.

The VPN Concentrator itself includes an IP routing subsystem with static routing, RIP (Routing Information Protocol), and OSPF (Open Shortest Path First) functions. RIP and OSPF are routing protocols that routers use for messages to other routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic.

Once the IP routing subsystem establishes the data paths, the routing itself occurs at wire speed. The subsystem looks at the destination IP address in all packets coming through the VPN Concentrator, even tunneled ones, to determine where to send them. If the packets are encrypted, it sends them to the appropriate tunneling protocol subsystem (PPTP, L2TP, IPSec) for processing and subsequent routing. If the packets are not encrypted, it routes them according to the configured IP routing parameters.

To route packets, the subsystem uses learned routes first (learned from RIP and OSPF), then static routes, then uses the default gateway. If you don't configure the default gateway, the subsystem drops packets that it can't otherwise route. The VPN Concentrator also provides a tunnel default gateway, which is a separate default gateway for tunneled traffic only.

You configure static routes, the default gateways, and system-wide OSPF parameters in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) parameters. You configure RIP and interface-specific OSPF parameters on the network interfaces; see **Configuration | Interfaces**.

This section of the Manager also lets you configure VPN Concentrator redundancy using VRRP (Virtual Router Redundancy Protocol). This feature applies to installations of two or more VPN Concentrators in a parallel, redundant configuration. It provides automatic switchover to a backup system in case the primary system is out of service, thus assuring user access to the VPN. This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

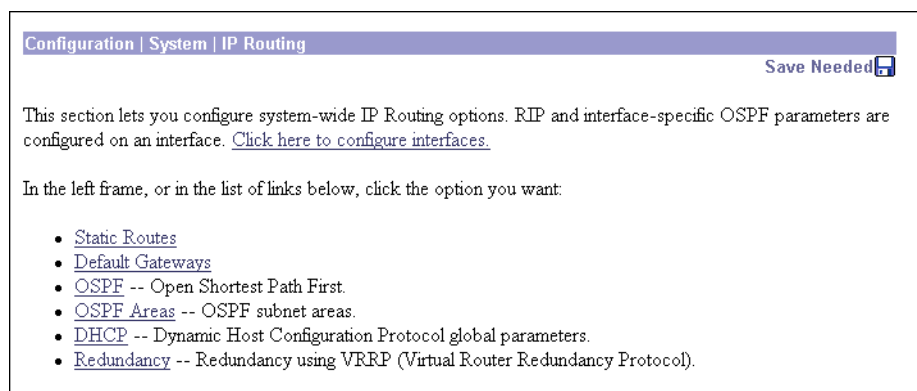
Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters.

- **Static Routes:** manually configured routing tables.
- **Default Gateways:** routes for otherwise unrouted traffic.
- **OSPF:** Open Shortest Path First routing protocol.
- **OSPF Areas:** subnet areas within the OSPF domain.
- **DHCP:** Dynamic Host Configuration Protocol global parameters.
- **Redundancy:** Virtual Router Redundancy Protocol parameters.

You configure RIP and interface-specific OSPF parameters on the network interfaces; click the highlighted link to go to the **Configuration | Interfaces** screen.

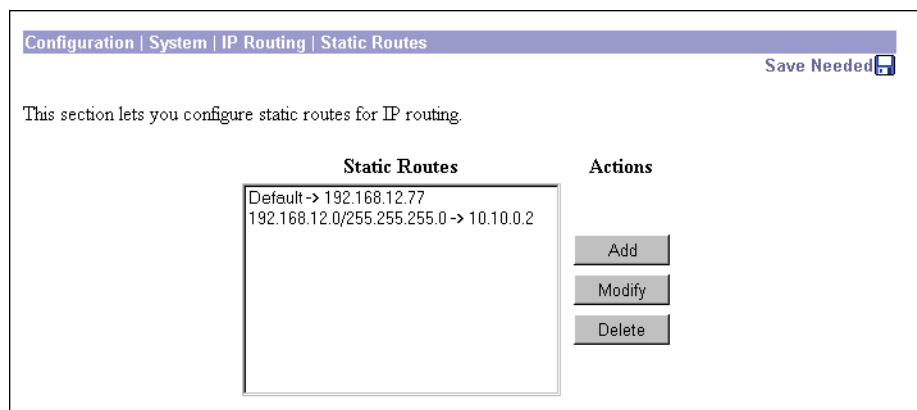
Figure 8-1: Configuration | System | IP Routing screen



Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing. You usually configure static routes for private networks that cannot be learned via RIP or OSPF.

Figure 8-2: Configuration | System | IP Routing | Static Routes screen



Static Routes

The **Static Routes** list shows manual IP routes that have been configured. The format is [destination network address/subnet mask -> outbound destination]; e.g., 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as [Default -> default router address]. If no static routes have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the **Configuration | System | IP Routing | Static Routes | Add** screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the **Configuration | System | IP Routing | Static Routes | Modify** screen. If you select the default gateway, the Manager opens the **Configuration | System | IP Routing | Default Gateways** screen.

To delete a configured static route, select the route from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the **Configuration | System | IP Routing | Default Gateways** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

Add: Configure and add a new static, or manual, route to the IP routing table.

Modify: Modify the parameters for a configured static route.

Figure 8-3: Configuration | System | IP Routing | Static Routes | Add or Modify screen

The screenshot shows two overlapping windows from the Manager interface. The top window is titled "Configuration | System | IP Routing | Static Routes | Modify" and contains the text "Modify a configured static route." The bottom window is titled "Configuration | System | IP Routing | Static Routes | Add" and contains the text "Configure and add a static route." Below this text are several input fields and instructions:

- Network Address:** An input field with the instruction "Enter the network address."
- Subnet Mask:** An input field with the instruction "Enter the subnet mask."
- Metric:** An input field with the instruction "Enter the numeric metric for this route (1 through 16)."
- Destination:** A section header for the following field.
- Router Address:** An input field with the instruction "Enter the router/gateway IP address."
- Interface:** A dropdown menu currently showing "Ethernet1 (Private) (10.10.147.2)" with the instruction "Select the interface to route to."

At the bottom of the "Add" window are two buttons: "Add" and "Cancel".

Network Address

Enter the destination network IP address that this static route applies to. Packets with this destination address will be sent to the **Destination** below. Used dotted decimal notation; e.g., 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address, using dotted decimal notation (e.g., 255.255.255.0). The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

Enter the metric, or cost, for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Destination

Click a radio button to select the outbound destination for these packets. You can select only one destination: either a specific router/gateway, or a VPN Concentrator interface.

Router Address

Enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN Concentrator and the packet's ultimate destination. Use dotted decimal notation; e.g., 10.10.0.2.

Interface

Click the drop-down menu button and select a configured VPN Concentrator interface as the outbound destination. The menu lists all interfaces that have been configured.

For example, in a LAN-to-LAN configuration where remote-access clients are assigned IP addresses that aren't on the private network, you could configure a static route with those addresses outbound to the Ethernet 1 (Private) interface. The clients could then access the peer VPN Concentrator and its networks.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the **Configuration | System | IP Routing | Static Routes** screen. Any new route appears at the bottom of the **Static Routes** list.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing | Static Routes** screen, and the **Static Routes** list is unchanged.

Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing, and configure the tunnel default gateway for tunneled traffic. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the **Configuration | Quick | System Info** screen.

The IP routing subsystem routes data packets first using learned routes, then static routes, then the default gateway. If you don't specify a default gateway, the system drops packets it can't otherwise route.

For tunneled data, if the system doesn't know a destination address it tries to route the packet to the tunnel default gateway first. If that route isn't configured, it uses the regular default gateway.

Figure 8-4: Configuration | System | IP Routing | Default Gateways screen

Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation; e.g., 192.168.12.77. This address must *not* be the same as the IP address configured on any VPN Concentrator interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

To delete a configured default gateway, enter 0.0.0.0.

The default gateway must be reachable from a VPN Concentrator interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if this route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Tunnel Default Gateway

Enter the IP address of the default gateway for tunneled data. Use dotted decimal notation; e.g., 10.10.0.2. If you do not use a tunnel default gateway, enter 0.0.0.0 (the default entry).

To delete a configured tunnel default gateway, enter 0.0.0.0.

This gateway is often a firewall in parallel with the VPN Concentrator and between the public and private networks. The tunnel default gateway applies to all tunneled traffic, including IPSec LAN-to-LAN traffic.

Note: If you use an external device instead of the VPN Concentrator for NAT (Network Address Translation), you must configure the tunnel default gateway.

Override Default Gateway

To allow default gateways learned via RIP or OSPF to override the configured **Default Gateway**, check the box (the default). To always use the configured **Default Gateway**, clear the box.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen. If you configure a **Default Gateway**, it also appears in the **Static Routes** list on the **Configuration | System | IP Routing | Static Routes** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

Configuration | System | IP Routing | OSPF

This screen lets you configure system-wide parameters for the OSPF (Open Shortest Path First) routing protocol. You must also configure interface-specific OSPF parameters on the **Configuration | Interfaces** screens.

OSPF is a protocol that the IP routing subsystem uses for messages to other OSPF routers within an internal or private network, to determine network connectivity, status, and optimum paths for sending data traffic. The VPN Concentrator supports OSPF version 2 (RFC 2328).

The complete private network is called an OSPF Autonomous System (AS), or domain. The subnets within the AS are called areas. You configure OSPF areas on the **Configuration | System | IP Routing | OSPF Areas** screens.

Figure 8-5: Configuration | System | IP Routing | OSPF screen

Configuration | System | IP Routing | OSPF

Configure system-wide parameters for OSPF (Open Shortest Path First) IP routing protocol.

Enabled Check to enable OSPF.

Router ID Enter the Router ID.

Autonomous System Check to indicate that this is an Autonomous System boundary router.

Apply Cancel

Enabled

To enable the VPN Concentrator OSPF router, check the box. (By default it is not checked.) You must also enter a **Router ID** below. You must check this box for OSPF to work on any interface that uses it.

To change a configured **Router ID** below, you must disable OSPF here.

To enable OSPF routing on an interface, you must also configure and enable OSPF on the appropriate **Configuration | Interfaces** screen.

Router ID

The router ID uniquely identifies the VPN Concentrator OSPF router to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network.

Enter the router ID in the field, using dotted decimal IP address format (e.g., 10.10.4.6). The default entry is 0.0.0.0 (no router configured). If you enable the OSPF router, you must enter an ID.

Once you configure and apply a router ID, you must disable OSPF above before you can change it. You cannot change the ID back to 0.0.0.0.

Autonomous System

An OSPF Autonomous System (AS), or domain, is a complete internal network. An AS boundary router exchanges routing information with routers belonging to other Autonomous Systems, and advertises external AS routing information throughout its AS.

Check the box to indicate that the VPN Concentrator OSPF router is the boundary router for an Autonomous System. If you check this box, the VPN Concentrator also redistributes RIP and static routes into the OSPF areas. By default, the box is not checked.

Apply / Cancel

To apply your OSPF settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

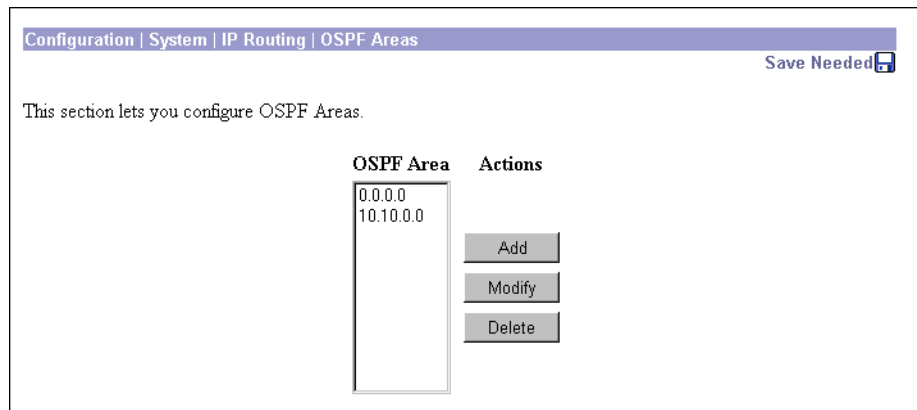
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

Configuration | System | IP Routing | OSPF Areas

This section of the Manager lets you configure OSPF areas, which are the subnets within an OSPF Autonomous System or domain. You should configure entries for all areas connected to this VPN Concentrator OSPF router.

You can also identify an OSPF area on a VPN Concentrator network interface (see **Configuration | Interfaces**). Those area identifiers appear in the **OSPF Area** list on this screen.

Figure 8-6: Configuration | System | IP Routing | OSPF Areas screen



OSPF Area

The **OSPF Area** list shows identifiers for all areas that are connected to this VPN Concentrator OSPF router. The format is the same as a dotted decimal IP address; e.g., 10.10.0.0. The default entry is 0.0.0.0, which identifies a special area—the backbone—that contains all area border routers, which are the routers connected to multiple areas.

Add / Modify / Delete

To configure and add a new OSPF area, click **Add**. The Manager opens the **Configuration | System | IP Routing | OSPF Areas | Add** screen.

To modify a configured OSPF area, select the area from the list and click **Modify**. The Manager opens the **Configuration | System | IP Routing | OSPF Areas | Modify** screen.

To delete a configured OSPF area, select the area from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **OSPF Area** list.

Reminder: The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | IP Routing | OSPF Areas | Add or Modify

These Manager screens let you:

Add: Configure and add an OSPF area.

Modify: Modify parameters for a configured OSPF area.

Note: Once you have configured an OSPF Area, you cannot modify its ID. To change an area ID, delete the existing area and add a new one.

Figure 8-7: Configuration | System | IP Routing | OSPF Areas | Add or Modify screen

Area ID

Add: Enter the area ID in the field using IP address dotted decimal notation; e.g., 10.10.0.0. The default entry is 0.0.0.0, the backbone.

Modify: Once you have configured an area ID, you cannot change it. See note above.

The **Area ID** identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. The 0.0.0.0 area ID identifies a special area—the backbone—that contains all area border routers.

Area Summary

Check the box to have the OSPF router generate and propagate summary LSAs (Link-State Advertisements) into OSPF stub areas. LSAs describe the state of the router's interfaces and routing paths. Stub areas contain only final-destination hosts and do not pass traffic through to other areas. Sending LSAs to them is usually not necessary. By default this box is not checked.

External LSA Import

Click the drop-down menu button and select whether to bring in LSAs from neighboring Autonomous Systems. LSAs describe the state of the AS router's interfaces and routing paths. Importing those LSAs builds a more complete link-state database, but it requires more processing. The choices are:

External = Yes, import LSAs from neighboring ASs (the default).

No External = No, do not import external LSAs.

Add or Apply / Cancel

To add this OSPF area to the list of configured areas, click **Add**. Or to apply your changes to this OSPF area, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | IP Routing | OSPF Areas** screen. Any new entry appears at the bottom of the **OSPF Area** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing | OSPF Areas** screen, and the **OSPF Area** list is unchanged.

Configuration | System | IP Routing | DHCP

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) parameters that apply to DHCP functions within the VPN Concentrator. You can use external DHCP servers to assign IP addresses to clients as a VPN tunnel is established.

If you check **Use DHCP** on the **Configuration | System | Address Management | Assignment** screen, you must configure at least one DHCP server on the **Configuration | System | Servers | DHCP** screens. You configure global DHCP parameters here.

Figure 8-8: Configuration | System | IP Routing | DHCP screen

Configuration | System | IP Routing | DHCP

Configure system-wide DHCP (Dynamic Host Configuration Protocol) parameters.

Enabled Check to enable DHCP.

Lease Timeout minutes

Listen Port *We recommend that you not change this default.*

Timeout Period seconds

Enabled

Check the box to enable DHCP functions within the VPN Concentrator. The box is checked by default. To use DHCP address assignment, you must enable DHCP functions here.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from a DHCP server. Minimum is 5, default is 120, maximum is 500000 minutes. DHCP servers “lease” IP addresses for this period of time. Before the lease expires, the VPN Concentrator asks to renew it on behalf of the client. If for some reason the lease is not renewed, the connection terminates when the lease expires. The DHCP server’s lease period takes precedence over this setting.

Listen Port

Enter the UDP port number on which DHCP server response messages are accepted. The default is 67, which is the well-known port. *To ensure proper communication with DHCP servers, we strongly recommend that you not change this default.*

Timeout Period

Enter the initial time in seconds to wait for a response to a DHCP request before sending the request to the next configured DHCP server. Minimum is 1, default is 2, maximum is 10 seconds. This time doubles with each cycle through the list of configured DHCP servers.

Apply / Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

Configuration | System | IP Routing | Redundancy

This screen lets you configure parameters for Virtual Router Redundancy Protocol (VRRP), which manages automatic switchover from one VPN Concentrator to another in a redundant installation. Automatic switchover provides user access to the VPN even if one VPN Concentrator is out of service for some reason; e.g., system crash, power failure, hardware failure, physical interface failure, system shutdown or reboot.

These functions apply only to installations where two or more VPN Concentrators are in parallel, with the Public interfaces of all systems on a common LAN and with the Private and/or External interfaces of all systems on different common LANs. One VPN Concentrator is the Master system, and the others are Backup systems. A Backup system acts as a virtual Master system when a switchover occurs.

VRRP works only on LAN (Ethernet) interfaces, not on WAN interfaces.

This feature supports user access via IPSec LAN-to-LAN connections, IPSec client (single-user remote-access) connections, and PPTP client connections.

- For IPSec LAN-to-LAN connections, switchover is fully automatic. Users need do nothing.
- For single-user IPSec and PPTP connections, users are disconnected from the failing system but they can reconnect without changing any connection parameters.

Switchover typically occurs within 3 to 10 seconds.

Notes: Before configuring or enabling VRRP on this screen, you must configure all Ethernet interfaces that apply to your installation, on all redundant VPN Concentrators. See the **Configuration | Interfaces** screens.

You must also configure *identical* IPSec LAN-to-LAN parameters on the redundant VPN Concentrators. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screens.

Figure 8-9: Configuration | System | IP Routing | Redundancy screen

Configuration | System | IP Routing | Redundancy

Configure the Virtual Router Redundancy Protocol (VRRP) for your system. **All interfaces that you want to configure VRRP on should already be configured.** If you later configure an additional interface, you need to revisit this screen.

Enable VRRP <input type="checkbox"/>	Check to enable VRRP.
Group ID <input style="width: 100px;" type="text" value="1"/>	Enter the Group ID for this set of redundant routers.
Group Password <input style="width: 100px;" type="text"/>	Enter the shared group password, or leave blank for no password.
Role <input style="width: 50px;" type="text" value="Master"/>	Select the Role for this system within the group.
Advertisement Interval <input style="width: 100px;" type="text" value="1"/>	Enter the Advertisement interval (seconds).
Group Shared Addresses	
1 (Private) <input style="width: 100px;" type="text" value="100.200.147.2"/>	
2 (Public) <input style="width: 100px;" type="text" value="192.168.12.34"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Enable VRRP

Check this box to enable VRRP functions. The box is not checked by default.

Group ID

Enter a number that uniquely identifies this group of redundant VPN Concentrators. This number must be the same on all systems in this group. Use a number from 1 (default) to 255. Since there is rarely more than one virtual group on a LAN, we suggest you accept the default.

Group Password

Enter a password for additional security in identifying this group of redundant VPN Concentrators. Maximum 8 characters. The Manager shows your entry in clear text, and VRRP advertisements contain this password in clear text. This password must be the same on all systems in this group. Leave this field blank to use no password.

Role

Click the drop-down menu button and select the role of this VPN Concentrator in this redundant group.

Master = This is the Master system in this group (the default selection). Be sure to configure *only one* Master system in a group with a given **Group ID**.

Backup 1 through **Backup 5** = This is a Backup system in this group.

Advertisement Interval

Enter the time interval in seconds between VRRP advertisements to other systems in this group. Only the Master system sends advertisements; this field is ignored on Backup systems while they remain Backup. Minimum is 1 (default), maximum is 255 seconds. Since a Backup system can become a Master system, we suggest you accept the default for all systems.

Group Shared Addresses

Enter the IP addresses that are treated as configured router addresses by all virtual routers in this group. The Manager displays fields only for the Ethernet interfaces that have been configured.

On the Master system, these entries are the IP addresses configured on its Ethernet interfaces, and the Manager supplies them by default.

On a Backup system, the fields are empty by default, and you must enter the same IP addresses as those on the *Master* system.

1 (Private)

The IP address for the Ethernet 1 (Private) interface shared by the virtual routers in this group.

2 (Public)

The IP address for the Ethernet 2 (Public) interface shared by the virtual routers in this group.

3 (External)

The IP address for the Ethernet 3 (External) interface shared by the virtual routers in this group.

Apply / Cancel

To apply the settings for VRRP, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | IP Routing** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | IP Routing** screen.

End of Chapter



Management Protocols

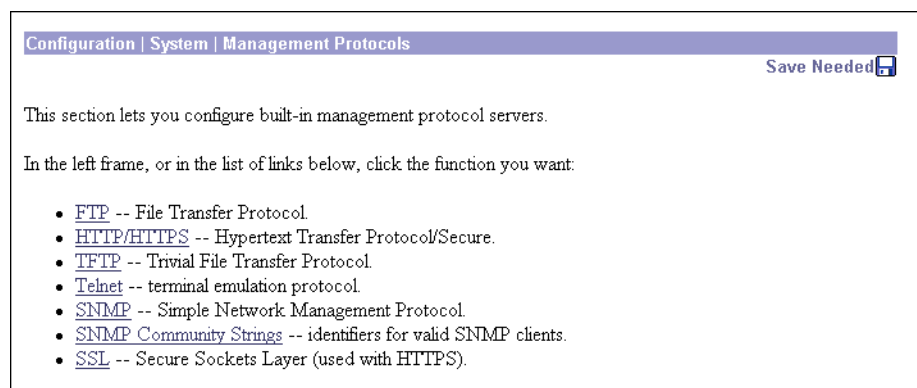
The VPN 3000 Concentrator Series includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN Concentrator servers that provide management functions using:

- **FTP:** File Transfer Protocol.
- **HTTP/HTTPS:** Hypertext Transfer Protocol, and HTTP over SSL (Secure Sockets Layer) protocol.
- **TFTP:** Trivial File Transfer Protocol.
- **Telnet:** terminal emulation protocol, and Telnet over SSL.
- **SNMP:** Simple Network Management Protocol.
- **SNMP Community Strings:** identifiers for valid SNMP clients.
- **SSL:** Secure Sockets Layer protocol.

Figure 9-1: Configuration | System | Management Protocols screen



Configuration | System | Management Protocols | FTP

This screen lets you configure and enable the VPN Concentrator's FTP (File Transfer Protocol) server. When the server is enabled, you can use an FTP client to upload and download files in VPN Concentrator flash memory.

FTP server login usernames and passwords are the same as those enabled and configured on the **Administration | Access Rights | Administrators** screens. To protect security, the VPN Concentrator does not allow anonymous FTP login.

The settings here have no effect on FTP backup of event log files (see **Configuration | System | Events | General** and **FTP Backup**). For those operations, the VPN Concentrator acts as an FTP client.

Figure 9-2: Configuration | System | Management Protocols | FTP screen

Configuration | System | Management Protocols | FTP

Configure the FTP server.

Enable Disabling will provide additional security.

Port The default port is 21. Changing the port will provide additional security.

Maximum Connections Enter the maximum number of concurrent control connections (sessions).

Enable

Check the box to enable the FTP server. The box is checked by default. Disabling the FTP server provides additional security.

Port

Enter the port number that the FTP server uses. The default is 21, which is the well-known port. Changing the port number provides additional security.

Maximum Connections

Enter the maximum number of concurrent control connections (sessions) that the FTP server allows. (FTP uses separate connections for control and data transfer during a session.) Minimum is 1, default is 5, maximum is 20.

Apply / Cancel

To apply your FTP server settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Configuration | System | Management Protocols | HTTP/HTTPS

This screen lets you configure and enable the VPN Concentrator's HTTP/HTTPS server: Hypertext Transfer Protocol and HTTP over SSL (Secure Sockets Layer) protocol. When the server is enabled, you can use a Web browser to communicate with the VPN Concentrator. HTTPS lets you use a Web browser over a secure, encrypted connection.

Notes: The VPN Concentrator Manager requires the HTTP/HTTPS server. *If you click **Apply**, even if you have made no changes on this screen, you will break your HTTP/HTTPS connection and you must restart the Manager session from the login screen.*

If you disable *either* HTTP or HTTPS, and that is the protocol you are currently using, you can reconnect with the other protocol if it is enabled and configured.

If you disable *both* HTTP and HTTPS, you cannot use a Web browser to connect to the VPN Concentrator. Use the Cisco Command Line Interface from the console or a Telnet session.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1, *Using the VPN 3000 Concentrator Series Manager*.
- To configure SSL parameters, see the **Configuration | System | Management Protocols | SSL** screen.
- To install, generate, view, or delete the SSL certificate on the VPN Concentrator, see the **Administration | Certificate Management** screens.

Figure 9-3: Configuration | System | Management Protocols | HTTP/HTTPS screen

Enable HTTP

Check the box to enable the HTTP server. The box is checked by default. You must enable HTTP to install the SSL certificate in the browser initially, so you can thereafter use HTTPS. Disabling the HTTP server provides additional security, but makes system management less convenient. See the notes above.

Enable HTTPS

Check the box to enable the HTTPS server. The box is checked by default. HTTPS—also known as HTTP over SSL—lets you use the VPN Concentrator Manager over an encrypted connection.

HTTP Port

Enter the port number that the HTTP server uses. The default is 80, which is the well-known port. Changing the port number provides additional security.

HTTPS Port

Enter the port number that the HTTPS server uses. The default is 443, which is the well-known port. Changing the port number provides additional security.

Maximum Sessions

Enter the maximum number of concurrent, combined HTTP and HTTPS sessions (users) that the server allows. Minimum is 1, default is 4, maximum is 10.

Apply / Cancel

To apply your HTTP/HTTPS server settings, to include your settings in the active configuration, *and to break the current HTTP/HTTPS connection*, click **Apply**. If HTTP or HTTPS is still enabled, the Manager returns to the main login screen. If both HTTP and HTTPS are disabled, you can no longer use the Manager.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Configuration | System | Management Protocols | TFTP

This screen lets you configure and enable the VPN Concentrator's TFTP (Trivial File Transfer Protocol) server. When the server is enabled, you can use a TFTP client to upload and download files in VPN Concentrator flash memory.

TFTP is similar to FTP, but it has no login procedure and no user interface commands. It allows only file transfers. The lack of a login procedure makes it relatively insecure.

The settings here have no effect on TFTP file transfer from the **Administration | File Management | TFTP Transfer** screen. For those operations, the VPN Concentrator acts as a TFTP client.

Figure 9-4: Configuration | System | Management Protocols | TFTP screen

Configuration | System | Management Protocols | TFTP

Configure the TFTP server.

Enable Disabling will provide additional security.

Port The default port is 69. Changing the port will provide additional security.

Maximum Connections Enter the maximum number of concurrent connections.

Timeout Enter the timeout in seconds for inactive connections. Change this value only if you have problems with TFTP.

Enable

Check the box to enable the TFTP server. The box is not checked by default. Disabling the TFTP server provides additional security.

Port

Enter the port number that the TFTP server uses. The default is 69, which is the well-known port. Changing the port number provides additional security.

Maximum Connections

Enter the maximum number of simultaneous connections that the TFTP server allows. Minimum is 1, default is 5, maximum is 20.

Timeout

Enter the timeout in seconds for inactive TFTP connections. Minimum is 1, default is 10, maximum is 30 seconds. Change the default value only if you have problems with TFTP transfers.

Apply / Cancel

To apply your TFTP settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Configuration | System | Management Protocols | Telnet

This screen lets you configure and enable the VPN Concentrator's Telnet terminal emulation server, and Telnet over SSL (Secure Sockets Layer protocol). When the server is enabled, you can use a Telnet client to communicate with the VPN Concentrator. You can fully manage and administer the VPN Concentrator using the Cisco Command Line Interface via Telnet.

Telnet server login usernames and passwords are the same as those enabled and configured on the **Administration | Access Rights | Administrators** screens.

Telnet/SSL uses a secure, encrypted connection. Although we are not aware of commercial Telnet/SSL clients, there are some working shareware applications. For example, see `ftp://ftp.gbnet.net/pub/security/Crypto/SSLapps` for `ssltel02.zip`, an "SSL Telnet for Windows" shareware application. *(Please note that we mention this application for information only and that Cisco Systems does not supply, support, or endorse it in any way.)*

See the **Configuration | System | Management Protocols | SSL** screen to configure SSL parameters. See the **Administration | Certificate Management | Certificates** screen to manage the SSL digital certificate.

Figure 9-5: Configuration | System | Management Protocols | Telnet screen

Configuration | System | Management Protocols | Telnet

Configure the Telnet server.

Enable Telnet Disabling will provide additional security.

Enable Telnet/SSL Telnet/SSL uses SSL encryption to provide security.

Telnet Port The default port is 23. Changing the port will provide additional security.

Telnet/SSL Port The default port is 992. Changing the port will provide additional security.

Maximum Connections Enter the maximum number of concurrent connections.

Apply Cancel

Enable Telnet

Check the box to enable the Telnet server. The box is checked by default. Disabling the Telnet server provides additional security, but doing so prevents using the Cisco Command Line Interface via Telnet.

Enable Telnet/SSL

Check the box to enable Telnet over SSL. The box is checked by default. Telnet/SSL uses Telnet over a secure, encrypted connection.

Telnet Port

Enter the port number that the Telnet server uses. The default is 23, which is the well-known port number. Changing the port number provides additional security.

Telnet/SSL Port

Enter the port number that Telnet over SSL uses. The default is 992, which is the well-known port number. Changing the port number provides additional security.

Maximum Connections

Enter the maximum number of concurrent, combined Telnet and Telnet/SSL connections that the server allows. Minimum is 1, default is 5, maximum is 10.

Apply / Cancel

To apply your Telnet settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Configuration | System | Management Protocols | SNMP

This screen lets you configure and enable the VPN Concentrator's SNMP (Simple Network Management Protocol) server. When the server is enabled, you can use an SNMP client to collect information from the VPN Concentrator but not to configure it.

To use the SNMP server, you must also configure an SNMP Community on the **Configuration | System | Management Protocols | SNMP Communities** screen.

The settings on this screen have no effect on sending system events to SNMP trap destinations (see **Configuration | System | Events | General** and **Trap Destinations**). For those functions, the VPN Concentrator acts as an SNMP client.

Figure 9-6: Configuration | System | Management Protocols | SNMP screen

Configuration | System | Management Protocols | SNMP

Configure the SNMP server.

Enable Disabling will provide additional security. You can use third-party SNMP managers only for viewing statistics, not for configuring this device.

Port The default port is 161. Changing the port will provide additional security.

Maximum Queued Requests Enter the maximum number of outstanding queued requests.

Enable

Check the box to enable the SNMP server. The box is checked by default. Disabling the SNMP server provides additional security.

Port

Enter the port number that the SNMP server uses. The default is 161, which is the well-known port number. Changing the port number provides additional security.

Maximum Queued Requests

Enter the maximum number of outstanding queued requests that the SNMP server allows. Minimum is 1, default is 4, maximum is 200.

Apply / Cancel

To apply your SNMP settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

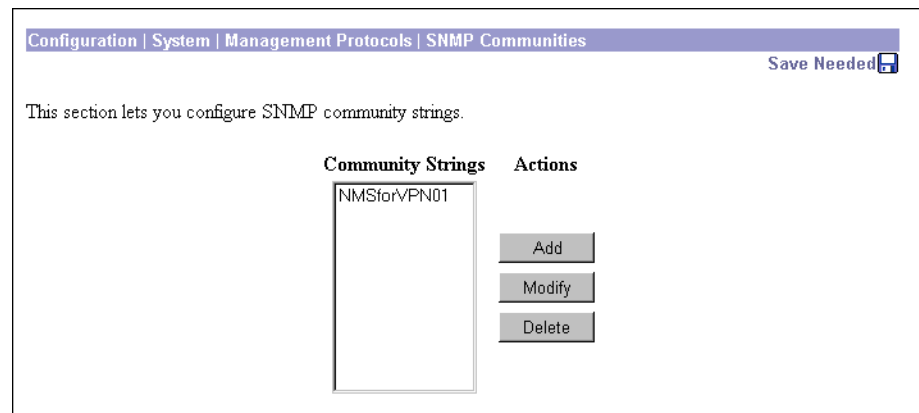
*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Configuration | System | Management Protocols | SNMP Communities

This section of the Manager lets you configure and manage SNMP community strings, which identify valid communities from which the SNMP server will accept requests. A community string is like a password: it validates messages between an SNMP client and the server.

To use the VPN Concentrator SNMP server, you must configure and add at least one community string. You can configure a maximum of 10 community strings. To protect security, the SNMP server does *not* include the usual default `public` community string, and we recommend that you not configure it.

Figure 9-7: Configuration | System | Management Protocols | SNMP Communities screen

Community Strings

The **Community Strings** list shows SNMP community strings that have been configured. If no strings have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new community string, click **Add**. The Manager opens the **Configuration | System | Management Protocols | SNMP Communities | Add** screen.

To modify a configured community string, select the string from the list and click **Modify**. The Manager opens the **Configuration | System | Management Protocols | SNMP Communities | Modify** screen.

To delete a configured community string, select the string from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Management Protocols | SNMP Communities | Add or Modify

These Manager screens let you:

Add: Configure and add a new SNMP community string.

Modify: Modify a configured SNMP community string.

Figure 9-8: Configuration | System | Management Protocols | SNMP Communities | Add or Modify screen

Community String

Enter the SNMP community string. Maximum 31 characters, case-sensitive.

Add or Apply / Cancel

To add this entry to the list of configured community strings, click **Add**. Or to apply your changes to this community string, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Management Protocols | SNMP Communities** screen; a new entry appears at the bottom of the **Community Strings** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry or changes, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols | SNMP Communities** screen, and the **Community Strings** list is unchanged.

Configuration | System | Management Protocols | SSL

This screen lets you configure the VPN Concentrator SSL (Secure Sockets Layer) protocol server. These settings apply to both HTTPS and Telnet over SSL. HTTPS lets you use a Web browser over a secure, encrypted connection to manage the VPN Concentrator.

SSL creates a secure session between the client and the VPN Concentrator server. The client first authenticates the server, they negotiate session security parameters, and then they encrypt all data passed during the session. If, during negotiation, the server and client cannot agree on security parameters, the session terminates.

SSL uses digital certificates for authentication. The VPN Concentrator creates a self-signed SSL server certificate when it boots; or you can install in the VPN Concentrator an SSL certificate that has been

issued in a PKI context. This certificate must then be installed in the client (for HTTPS; Telnet doesn't usually require it). You need to install the certificate from a given VPN Concentrator only once.

The default SSL settings should suit most administration tasks and network security requirements. *We recommend that you not change them unadvisedly.*

Note: To ensure the security of your connection to the VPN Concentrator Manager, if you click **Apply** on this screen—even if you have made no changes—you will break your connection to the Manager and you must restart the Manager session from the login screen.


Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1, *Using the VPN 3000 Concentrator Series Manager*.
- To configure HTTPS parameters, see the **Configuration | System | Management Protocols | HTTP/HTTPS** screen.
- To configure Telnet/SSL parameters, see the **Configuration | System | Management Protocols | Telnet** screen.
- To manage SSL digital certificates, see the **Administration | Certificate Management** screens.

Figure 9-9: Configuration | System | Management Protocols | SSL screen

Configuration | System | Management Protocols | SSL

Configure SSL.

 If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Encryption Protocols

- RC4-128/MD5
- 3DES-168/SHA
- DES-56/SHA
- RC4-40/MD5 Export
- DES-40/SHA Export

Check the encryption algorithms to enable. Unchecking them all disables SSL.

Client Authentication

Check to enable client authentication. Client authentication requires an installed Certificate Authority and a personal certificate installed in your browser.

SSL Version

Select the SSL version to use. Using a SSL V2 Hello provides compatibility with most browsers.

Generated Certificate Key Size

Select the key size used in the generated certificate.

Encryption Protocols

Check the boxes for the encryption algorithms that the VPN Concentrator SSL server can negotiate with a client and use for session encryption. All are checked by default. You must check at least one algorithm to enable SSL. *Unchecking all algorithms disables SSL.*

The algorithms are negotiated in the order shown. You cannot change the order, but you can enable or disable selected algorithms.

RC4-128/MD5 = RC4 encryption with a 128-bit key and the MD5 hash function. This option is available in most SSL clients.

3DES-168/SHA = Triple-DES encryption with a 168-bit key and the SHA-1 hash function. This is the strongest (most secure) option.

DES-56/SHA = DES encryption with a 56-bit key and the SHA-1 hash function.

RC4-40/MD5 Export = RC4 encryption with a 128-bit key—40 bits of which are private—and the MD5 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.

DES-40/SHA Export = DES encryption with a 56-bit key—40 bits of which are private—and the SHA-1 hash function. This option is available in the export (non-U.S.) versions of many SSL clients.

Client Authentication

This parameter applies to HTTPS only; it is ignored for Telnet/SSL.

Check the box to enable SSL client authentication. The box is not checked by default. In the most common SSL connection, the client authenticates the server, not vice-versa. Client authentication requires personal certificates installed in the browser, and trusted certificates installed in the server. Specifically, the VPN Concentrator must have a root CA certificate installed; and a certificate signed by one of the VPN Concentrator's trusted CAs must be installed in the Web browser. See **Administration | Certificate Management**.

SSL Version

Click the drop-down menu button and select the SSL version to use. SSL Version 3 has more security options than Version 2, and TLS (Transport Layer Security) Version 1 has more security options than SSL Version 3. Some clients that send an SSL Version 2 "Hello" (initial negotiation), can actually use a more secure version during the session. Telnet/SSL clients usually can use only SSL Version 2.

Choices are:

Negotiate SSL V2/V3 = The server tries to use SSL Version 3 but accepts Version 2 if the client can't use Version 3. This is the default selection. This selection works with most browsers and Telnet/SSL clients.

SSL V3 with SSL V2 Hello = The server insists on SSL Version 3 but accepts an initial Version 2 "Hello."

SSL V3 Only = The server insists on SSL Version 3 only.

SSL V2 Only = The server insists on SSL Version 2 only. This selection works with most Telnet/SSL clients.

TLS V1 Only = The server insists on TLS Version 1 only. At present, only Microsoft Internet Explorer 5.0 supports this option.

TLS V1 with SSL V2 Hello = The server insists on TLS Version 1 but accepts an initial SSL Version 2 “Hello.” At present, only Microsoft Internet Explorer 5.0 supports this option.

Generated Certificate Key Size

Click the drop-down menu button and select the size of the RSA key that the VPN Concentrator uses in its self-signed (generated) SSL server certificate. A larger key size increases security, but it also increases the processing necessary in all transactions over SSL. The increases vary depending on the type of transaction (encryption or decryption).

Choices are:

512-bit RSA Key = This key size provides sufficient security. It is the most common, and requires the least processing.

768-bit RSA Key = This key size provides normal security and is the default selection. It requires approximately 2 to 4 times more processing than the 512-bit key.

1024-bit RSA Key = This key size provides high security. It requires approximately 4 to 8 times more processing than the 512-bit key.

Apply / Cancel

To apply your SSL settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Management Protocols** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Management Protocols** screen.

End of Chapter



Events

An *event* is any significant occurrence within or affecting the VPN 3000 Concentrator such as an alarm, trap, error condition, network problem, task completion, threshold breach, or status change. The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. You can also specify that certain events trigger a console message, a UNIX syslog record, an email message, or an SNMP management system trap.

Event attributes include *class* and *severity level*.

Event class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. Table 10-1 describes the event classes.

Table 10-1: VPN Concentrator event classes

Class name	Class description (event source) (*Cisco-specific event class)
AUTH	Authentication*
AUTHDBG	Authentication debugging*
AUTHDECODE	Authentication protocol decoding*
BKPLN	WAN backplane driver*
CAPI	Cryptography subsystem*
CERT	Digital certificates subsystem
CONFIG	Configuration subsystem*
DHCP	DHCP subsystem
DHCPDBG	DHCP debugging*
DHCPDECODE	DHCP decoding*
DM	Data Movement subsystem*
DNS	DNS subsystem

Table 10-1: VPN Concentrator event classes (continued)

Class name	Class description (event source) (*Cisco-specific event class)
DNSDBG	DNS debugging*
DNSDECODE	DNS decoding*
EVENT	Event subsystem*
EVENTDBG	Event subsystem debugging*
EVENTMIB	Event MIB changes*
EXPANSIONCARD	Expansion card (module) subsystem
FILTER	Filter subsystem
FILTERDBG	Filter debugging*
FSM	Finite State Machine subsystem (for debugging)*
FTPD	FTP daemon subsystem
GENERAL	NTP subsystem and other general events
GRE	GRE subsystem
GREDBG	GRE debugging*
GREDECODE	GRE decoding*
HARDWAREMON	Hardware monitoring (fans, temperature, voltages, etc.)
HDLC	HDLC/SYNC driver for WAN module*
HTTP	HTTP subsystem
HWDIAG	Hardware diagnostics for WAN module*
IKE	ISAKMP/Oakley (IKE) subsystem
IKEDBG	ISAKMP/Oakley (IKE) debugging*
IKEDECODE	ISAKMP/Oakley (IKE) decoding*
IP	IP router subsystem
IPDBG	IP router debugging*
IPDECODE	IP packet decoding*
IPSEC	IP Security subsystem
IPSECDBG	IP Security debugging*
IPSECDECODE	IP Security decoding*
L2TP	L2TP subsystem
L2TPDBG	L2TP debugging*
L2TPDECODE	L2TP decoding*
MIB2TRAP	MIB-II trap subsystem: SNMP MIB-II traps*

Table 10-1: VPN Concentrator event classes (continued)

Class name	Class description (event source) (*Cisco-specific event class)
OSPF	OSPF subsystem
PPP	PPP subsystem
PPPDBG	PPP debugging*
PPPDECODE	PPP decoding*
PPTP	PPTP subsystem
PPTPDBG	PPTP debugging*
PPTPDECODE	PPTP decoding*
PSH	Operating system command shell*
PSOS	Embedded real-time operating system*
QUEUE	System queue*
REBOOT	System rebooting
RM	Resource Manager subsystem*
SMTP	SMTP event handling
SNMP	SNMP trap subsystem
SSL	SSL subsystem
SYSTEM	Buffer, heap, and other system utilities*
T1E1	T1/E1 ports on WAN module*
TCP	TCP subsystem
TELNET	Telnet subsystem
TELNETDBG	Telnet debugging*
TELNETDECODE	Telnet decoding*
TIME	System time (clock)
VRRP	VRRP subsystem
WAN	WAN module subsystem*

Note: The Cisco-specific event classes provide information that is meaningful only to Cisco engineering or support personnel. Also, the DBG and DECODE events require significant system resources and may seriously degrade performance. We recommend that you avoid logging these events unless Cisco requests it.

Event severity level

Severity level indicates how serious or significant the event is; i.e., how likely it is to cause unstable operation of the VPN concentrator, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. Table 10-2 describes the severity levels.

Table 10-2: VPN Concentrator event severity levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that may require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding
11	Packet Decode	Low-level packet header decoding
12	Packet Decode	Hex dump of header
13	Packet Decode	Hex dump of packet

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the **Information** category, Level 6 provides greater detail than Level 4 but doesn't necessarily include the same information as Level 4.

Logging higher-numbered severity levels degrades performance, since more system resources are used to log and handle these events.

Note: The Debug (7–9) and Packet Decode (10–13) severity levels are intended for use by Cisco engineering and support personnel. We recommend that you avoid logging these events unless Cisco requests it.

The VPN Concentrator, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the **Configuration | System | Events | General** screen, and you can configure specific events for special handling on the **Configuration | System | Events | Classes** screens.

Event log

The VPN Concentrator records events in an event log, which is stored in nonvolatile memory. Thus the event log persists even if the system is powered off. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. The log wraps when it is full; that is, newer events overwrite older events when the log is full.

For the event log, you can configure:

- Which event classes and severity levels to log.
- Whether to save the event log to a file in flash memory when it is full (when it wraps). And if so:
 - The format of the information in the saved log file.
 - Whether to automatically send a copy of the saved log file via FTP to a remote system.

Event log data

Each entry (record) in the event log consists of several fields including:

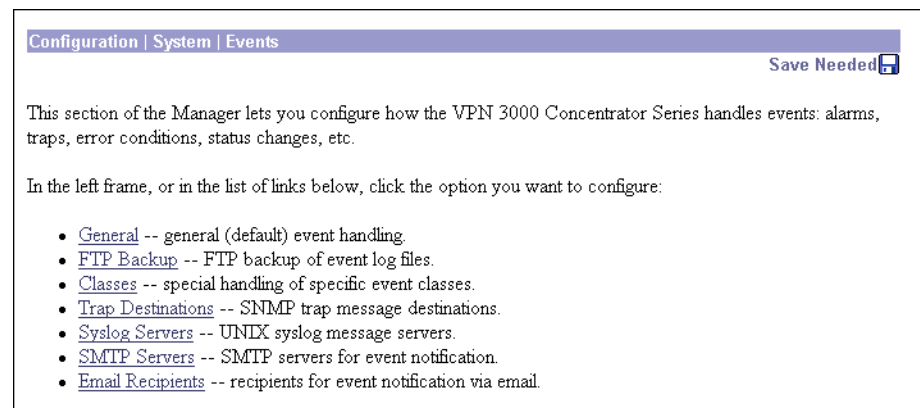
- A sequence number.
- Date and time.
- Event severity level.
- Event class and number.
- Event repetition count.
- Event IP address (only for certain events).
- Description string.

For more information, see the **Monitoring | Event Log** screen.

Configuration | System | Events

This section of the Manager lets you configure how the VPN Concentrator handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

Figure 10-1: Configuration | System | Events screen



Configuration | System | Events | General

This Manager screen lets you configure the general, or default, handling of all events. These defaults apply to all event classes.

You can override these default settings by configuring specific events for special handling on the **Configuration | System | Events | Classes** screens.

Figure 10-2: Configuration | System | Events | General screen

Configuration | System | Events | General

This section lets you configure default event handling.

Save Log on Wrap Check to save the event log to a file on wrap.

Save Log Format Multiline Select the format of the saved log files.

FTP Saved Log on Wrap Check to automatically FTP the saved log to a remote destination.

Email Source Address Enter the email address that appears in the **From:** field.

Syslog Format Original Select the format of Syslog messages.

Severity to Log 1-5 Select the range of severity values to enter in the log.

Severity to Console 1-3 Select the range of severity values to display on the console.

Severity to Syslog None Select the range of severity values to send to a Syslog server.

Severity to Email None Select the range of severity values to send via email to the recipient list.

Severity to Trap None Select the range of severity values to send to an SNMP system.

Apply Cancel

Save Log on Wrap

Check this box to automatically save the event log when it is full. (The box is not checked by default.) The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events. When the log is full, the entries wrap; that is, entry 2049 overwrites entry 1, etc.

If you select automatic save, the system saves the log file to a file in flash memory with the filename LOGNNNNN.TXT, where NNNNN is an increasing sequence number that starts with 00001 and restarts after 99999. The sequence numbers continue through reboots. For example, if four log files have already been saved, the next one saved after a reboot is LOG00005.TXT.

If flash memory has less than 2.56 MB of free space, the system deletes the oldest log file(s) to make room for the newest saved log file. It also generates an event that notes the deletion. If there are no old log files to delete, the save function fails, and the system generates an event that notes the failure.

Each saved log file requires about 334 KB. To conserve space in flash memory, we recommend that you periodically remove the saved log files. Keeping more than 10 to 12 files wastes space. The **Administration | File Management | Files** screen shows total, used, and free space in flash memory.

Note: The VPN Concentrator automatically saves the log file if it crashes, and when it is rebooted, regardless of this **Save Log on Wrap** setting. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging.

You can manage saved log files with options on this screen and on the **Administration | File Management** screens.

Save Log Format

Click the drop-down menu button to specify the format of the saved log files.

Multiline = Entries are ASCII text and appear on multiple 80-character lines (default). Choose this format for easiest reading and printing.

Comma Delimited = Each entry is a single record with fields separated by commas. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.

Tab Delimited = Each entry is a single record with fields separated by tab characters. Choose this format for subsequent processing by an application program such as a spreadsheet or accounting system.

See **Monitoring | Event Log** for details on event log fields.

FTP Saved Log on Wrap

Check this box to automatically send the saved event log file, when it wraps, via FTP to a remote computer. (The box is not checked by default.) To use this option, you must also check **Save Log on Wrap** above. This option *copies* the log file but does not delete it from the VPN Concentrator. If you check this box, you must also configure FTP destination system parameters on the **Configuration | System | Events | FTP Backup** screen.

Email Source Address

Enter the address to put in the **From:** field of an emailed event message. Enter up to 48 alphanumeric characters with no spaces; e.g., VPN07@altiga.com. You should configure this field if you configure any **Severity to Email** events; if you leave it blank, the **From:** field has the same address as the **To:** field (the recipient's email address).

Syslog Format

Click the drop-down menu button and select the format for all events sent to UNIX syslog servers. Choices are:

Original = Original VPN Concentrator event format with information on one line.

Cisco IOS Compatible = Event format that is compatible with Cisco syslog management applications.

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-5**: all events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-3**: all events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server by default. Choices are: **None, 1, 1-2, 1-3, ..., 1-6**. The default is **None**: no events are sent to a syslog server.

If you select any severity levels to send, you must also configure the syslog server(s) on the **Configuration | System | Events | Syslog Servers** screens.

Severity to Email

Click the drop-down menu button and select the range of event severity levels to email to recipients by default. Choices are: **None, 1, 1-2, 1-3**. The default is **None**: no events are sent via email.

If you select any severity levels to email, you must also configure an SMTP server on the **Configuration | System | Events | SMTP Servers** screens, and you must configure email recipients on the **Configuration | System | Events | Email Recipients** screens. You should also configure the **Email Source Address** above.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system by default. Event messages sent to SNMP systems are called “traps.” Choices are: **None, 1, 1-2, 1-3**. The default is **None**: no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the **Configuration | System | Events | Trap Destinations** screens.

The VPN Concentrator can send the standard, or “well-known,” SNMP traps listed in Table 10-3. To have an SNMP NMS receive them, you must configure the events as in the table, and configure a trap destination.

Table 10-3: Configuring “well-known” SNMP traps

To send this “well-known” SNMP trap	Configure either General event handling or this Event Class	With this Severity to Trap
coldStart	EVENT	1 or higher
linkDown	IP	1-3 or higher
linkUp	IP	1-3 or higher
authFailure (This trap is SNMP authentication failure, not tunnel authentication failure.)	SNMP	1-3 or higher

Apply / Cancel

To include your settings for default event handling in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Events** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events** screen.

Configuration | System | Events | FTP Backup

This screen lets you configure parameters for using FTP to automatically back up saved event log files on a remote computer. If you enable **FTP Saved Log on Wrap** on the **Configuration | System | Events | General** screen, you must configure the FTP parameters on this screen.

The VPN Concentrator acts as an FTP client when executing this function.

Figure 10-3: Configuration | System | Events | FTP Backup screen

Configuration | System | Events | FTP Backup

This screen lets you configure FTP backup options for the log.

FTP Server Enter the IP address or hostname of the destination FTP server.

FTP Directory Enter the directory pathname for files on the FTP server.

FTP Username Enter the username to log on to the FTP server.

FTP Password Enter the password to log on to the FTP server.

Verify Re-enter the password to verify it.

Apply Cancel

FTP Server

Enter the IP address or hostname of the destination computer to receive copies of saved event log files via FTP. (If you have configured a DNS server, you can enter a hostname; otherwise enter an IP address.)

FTP Directory

Enter the complete directory pathname on the destination computer to receive copies of saved event log files. For example, `c:\vpn\logfiles`.

FTP Username

Enter the username for FTP login on the destination computer.

FTP Password

Enter the password to use with the FTP username above. The field displays only asterisks.

Verify

Re-enter the FTP password to verify it. The field displays only asterisks.

Apply / Cancel

To include your FTP backup system settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | Events** screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

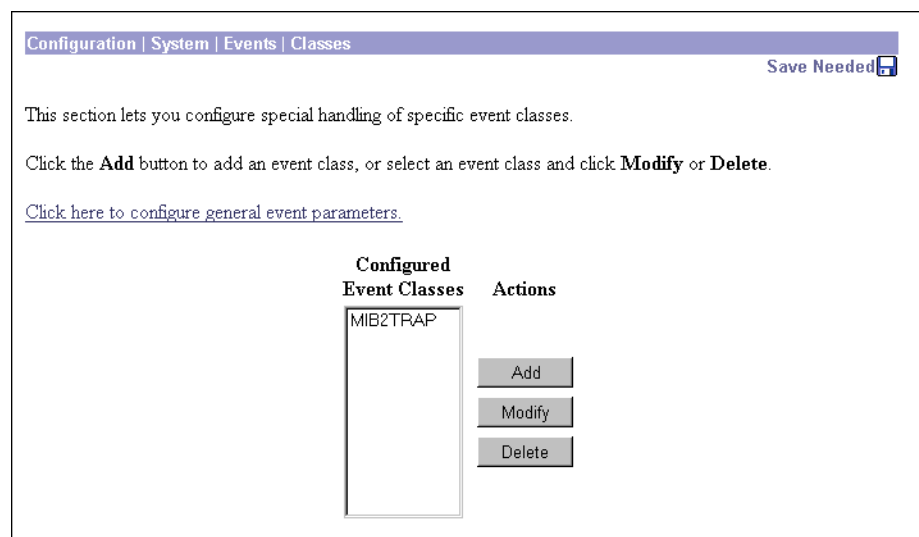
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events** screen.

Configuration | System | Events | Classes

This section of the Manager lets you add, configure, modify, and delete specific event classes for special handling. You can thus override the general, or default, handling of event classes. For example, you might want to send email for HARDWAREMON events of severity 1-2, whereas default event handling doesn't send any email.

Event classes denote the source of an event and refer to a specific hardware or software subsystem within the VPN Concentrator. Table 10-1 describes the event classes.

Figure 10-4: Configuration | System | Events | Classes screen



To configure default event handling, click the highlighted link that says “Click here to configure general event parameters.”

Configured Event Classes

The **Configured Event Classes** list shows the event classes that have been configured for special handling. The initial default entry is **MIB2TRAP**, which are SNMP MIB-II events, or “traps,” that you might want to monitor with an SNMP network management system. Other configured event classes are listed in

order by class number and name. If no classes have been configured for special handling, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new event class for special handling, click **Add**. See **Configuration | System | Events | Classes | Add**.

To modify an event class that has been configured for special handling, select the event class from the list and click **Modify**. See **Configuration | System | Events | Classes | Modify**.

To remove an event class that has been configured for special handling, select the event class from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Classes | Add or Modify

These screens let you:

Add and configure the special handling of a specific event class.

Modify the special handling of a specific event class.

Figure 10-5: Configuration | System | Events | Classes | Add or Modify screen

Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Configuration | System | Events | Classes | Add

This screen lets you add and configure an event class for special handling.

Class Name Select the event class to configure.

Enable Check to enable special handling of this class.

Severity to Log Select the range of severity values to enter in the log.

Severity to Console Select the range of severity values to display on the console.

Severity to Syslog Select the range of severity values to send to a Syslog server.

Severity to Email Select the range of severity values to send via email to the recipient list.

Severity to Trap Select the range of severity values to send to an SNMP system.

Add Cancel

Class Name

Add screen:

Click the drop-down menu button and select the event class you want to add and configure for special handling. (Please note that **Select Class** is an instruction reminder, not a class.) Table 10-1 describes the event classes.

Modify screen:

The field shows the configured event class you are modifying. You cannot change this field. All subsequent parameters on this screen apply to this event class only.

Enable

Check this box to enable the special handling of this event class. (The box is checked by default.)

Clearing this box lets you set up the parameters for the event class but activate it later, or temporarily disable special handling without deleting the entry. The **Configured Event Classes** list on the **Configuration | System | Events | Classes** screen indicates disabled event classes. Disabled event classes are handled according to the default parameters for all event classes.

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-5**: events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **1-3**: events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server. Choices are: **None, 1, 1-2, 1-3, ..., 1-13**. The default is **None**: no events are sent to a syslog server.

Note: Sending events to a syslog server generates IP packets, which can generate new events if this setting is above level 9. We strongly recommend that you keep this setting at or below level 6. Avoid setting this parameter above level 9.

If you select any severity levels to send, you must also configure the syslog server(s) on the **Configuration | System | Events | Syslog Servers** screens, and you should configure the **Syslog Format** on the **Configuration | System | Events | General** screen.

Severity to Email

Click the drop-down menu button and select the range of event severity levels to send to recipients via email. Choices are: **None**, **1**, **1-2**, **1-3**. The default is **None**: no events are sent via email.

If you select any severity levels to email, you must also configure an SMTP server on the **Configuration | System | Events | SMTP Servers** screen, and you must configure email recipients on the **Configuration | System | Events | Email Recipients** screens. You should also configure the **Email Source Address** on the **Configuration | System | Events | General** screen.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system. Event messages sent to SNMP systems are called “traps.” Choices are: **None**, **1**, **1-2**, **1-3**, **1-4**, **1-5**. The default is **None**: no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the **Configuration | System | Events | Trap Destinations** screens.

To configure “well-known” SNMP traps, see Table 10-3 under **Severity to Trap** for **Configuration | System | Events | General**.

Add or Apply / Cancel

To add this event class to the list of those with special handling, click **Add**. Or to apply your changes to this configured event class, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Classes** screen. Any new event class appears in the **Configured Event Classes** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events | Classes** screen.

Configuration | System | Events | Trap Destinations

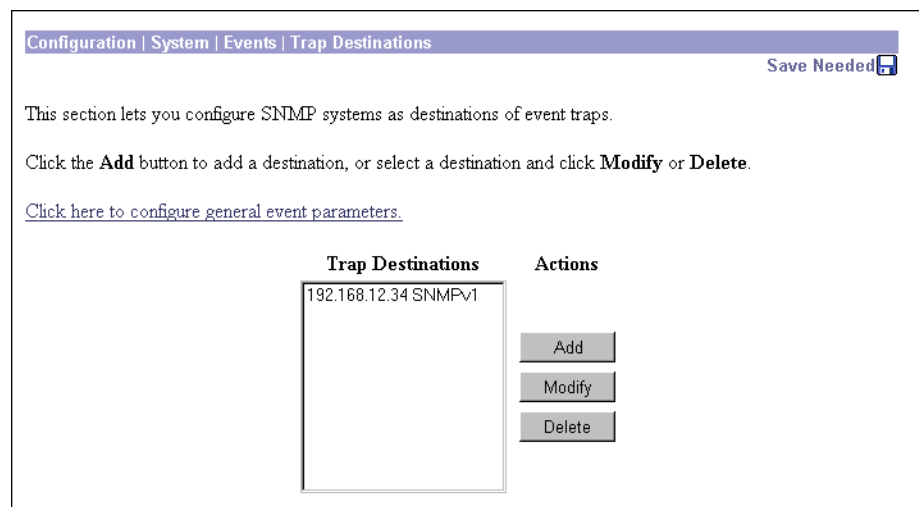
This section of the Manager lets you configure SNMP network management systems as destinations of event traps. Event messages sent to SNMP systems are called “traps.” If you configure any event handling—default or special—with values in **Severity to Trap** fields, you must configure trap destinations in this section.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

To configure “well-known” SNMP traps, see Table 10-3 under **Severity to Trap** for **Configuration | System | Events | General**.

To have an SNMP-based network management system (NMS) receive any events, you must also configure the NMS to “see” the VPN Concentrator as a managed device or “agent” in the NMS domain.

Figure 10-6: Configuration | System | Events | Trap Destinations screen



Trap Destinations

The **Trap Destinations** list shows the SNMP network management systems that have been configured as destinations for event trap messages, and the SNMP protocol version associated with each destination. If no trap destinations have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new SNMP trap destination, click **Add**. See **Configuration | System | Events | Trap Destinations | Add**.

To modify an SNMP trap destination that has been configured, select the destination from the list and click **Modify**. See **Configuration | System | Events | Trap Destinations | Modify**.

To remove an SNMP trap destination that has been configured, select the destination from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder: The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Configuration | System | Events | Trap Destinations | Add or Modify

These screens let you:

Add an SNMP destination system for event trap messages.

Modify a configured SNMP destination system for event trap messages.

Figure 10-7: Configuration | System | Events | Trap Destinations | Add or Modify screen

Destination

Enter the IP address or hostname of the SNMP network management system that is a destination for event trap messages. (If you have configured a DNS server, you can enter a hostname; otherwise enter an IP address.)

SNMP Version

Click the drop-down menu button and select the SNMP protocol version to use when formatting traps to this destination. Choices are **SNMPv1** (version 1; the default) and **SNMPv2** (version 2).

Community

Enter the community string to use in identifying traps from the VPN Concentrator to this destination. The community string is like a password: it validates messages between the VPN Concentrator and this NMS destination. If you leave this field blank, the default community string is `public`.

Port

Enter the UDP port number by which you access the destination SNMP server. Use a decimal number from 0 to 65535. The default is 162, which is the well-known port number for SNMP traps.

Add or Apply / Cancel

To add this system to the list of SNMP trap destinations, click **Add**. Or to apply your changes to this trap destination, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Trap Destinations** screen. Any new destination system appears in the **Trap Destinations** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

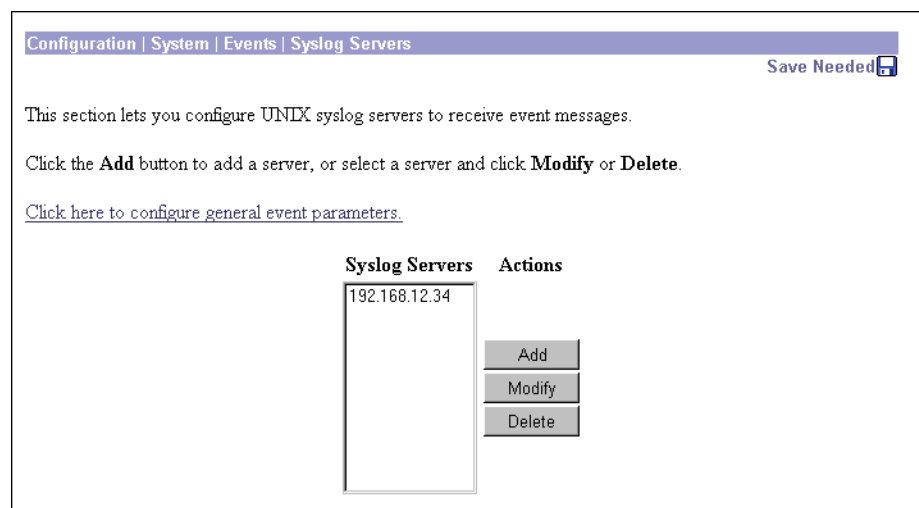
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | Events | Trap Destinations** screen, and the **Trap Destinations** list is unchanged.

Configuration | System | Events | Syslog Servers

This section of the Manager lets you configure UNIX syslog servers as recipients of event messages. Syslog is a UNIX daemon, or background process, that records events. The VPN Concentrator can send event messages in two syslog formats to configured syslog systems. If you configure any event handling—default or special—with values in **Severity to Syslog** fields, you must configure syslog servers in this section.

To configure default event handling and syslog formats, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

Figure 10-8: Configuration | System | Events | Syslog Servers screen



Syslog Servers

The **Syslog Servers** list shows the UNIX syslog servers that have been configured as recipients of event messages. You can configure a maximum of five syslog servers. If no syslog servers have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new syslog server, click **Add**. See **Configuration | System | Events | Syslog Servers | Add**.

To modify a syslog server that has been configured, select the server from the list and click **Modify**. See **Configuration | System | Events | Syslog Servers | Modify**.

To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Syslog Servers | Add or Modify

These screens let you:

Add a UNIX syslog server as a recipient of event messages. You can configure a maximum of five syslog servers.

Modify a configured UNIX syslog server that is a recipient of event messages.

Figure 10-9: Configuration | System | Events | Syslog Servers | Add or Modify screen

Syslog Server

Enter the IP address or hostname of the UNIX syslog server to receive event messages. (If you have configured a DNS server, you can enter a hostname; otherwise, enter an IP address.)

Port

Enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default is 514, which is the well-known port number.

Facility

Click the drop-down menu button and select the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. The choices are:

User = Random user-process messages.

Mail = Mail system.

Daemon = System daemons.

Auth = Security or authorization messages.

Syslog = Internal syslogd-generated messages.

LPR = Line printer subsystem.

News = Network news subsystem.

UUCP = UUCP (UNIX-to-UNIX Copy Program) subsystem.

Reserved (9) through **Reserved (14)** = Outside the **Local** range, with no name or assignment yet, but usable.

CRON = Clock daemon.

Local 0 through **Local 7** (default) = User defined.

Add or Apply / Cancel

To add this server to the list of syslog servers, click **Add**. Or to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Syslog Servers** screen. Any new server appears in the **Syslog Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

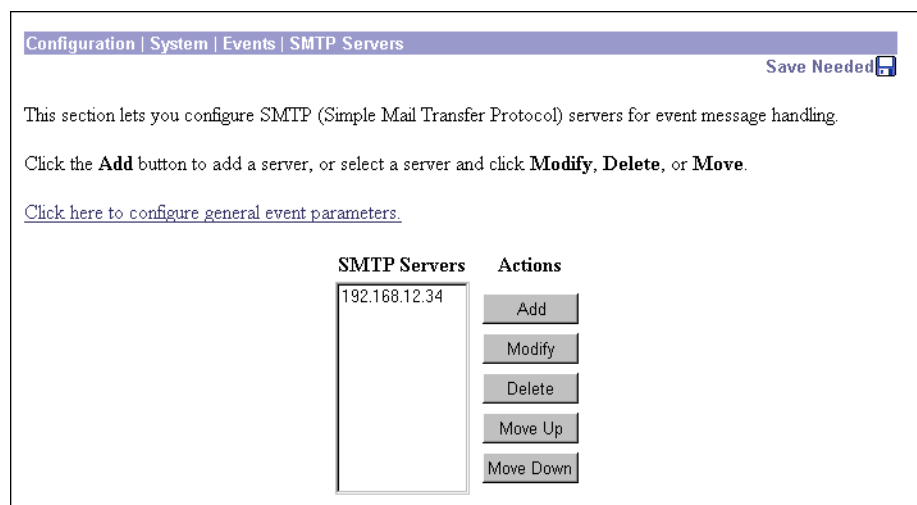
To discard your entries, click **Cancel**. The Manager returns to the **Configuration | System | Events | Syslog Servers** screen, and the **Syslog Servers** list is unchanged.

Configuration | System | Events | SMTP Servers

This section of the Manager lets you configure SMTP servers that you use to email event messages to email recipients. If you configure any event handling—default or special—with values in **Severity to Email** fields, you must identify at least one SMTP server to handle the outgoing email, and you must name at least one email recipient to receive the event messages. You can configure two SMTP servers: one primary and one backup in case the primary is unavailable.

To configure email recipients, see the **Configuration | System | Events | Email Recipients** screen.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

Figure 10-10: Configuration | System | Events | SMTP Servers screen

SMTP Servers

The **SMTP Servers** list shows the configured SMTP servers in the order in which the system accesses them. You can configure two prioritized SMTP servers so that you have a backup server in case the primary server is offline, congested, etc. If no SMTP servers have been configured, the list shows **--Empty--**.

Add / Modify / Delete / Move

To configure a new SMTP server, click **Add**. See **Configuration | System | Events | SMTP Servers | Add**.

To modify a configured SMTP server, select the server from the list and click **Modify**. See **Configuration | System | Events | SMTP Servers | Modify**.

To remove a configured SMTP server, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **SMTP Servers** list.

To change the order in which the system accesses configured SMTP servers, select the server from the list and click **Move** ↑ or **Move** ↓. The Manager refreshes the screen and shows the reordered **SMTP Servers** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | SMTP Servers | Add or Modify

These screens let you:

Add an SMTP server to the list of configured SMTP servers. You can configure two SMTP servers: a primary and a backup.

Modify the IP address or hostname of a configured SMTP server.

Figure 10-11: Configuration | System | Events | SMTP Servers | Add or Modify screen

The figure shows two overlapping screenshots of the configuration interface. The top screenshot shows the breadcrumb 'Configuration | System | Events | SMTP Servers | Modify' and the text 'Modify a configured SMTP server.' The bottom screenshot shows the breadcrumb 'Configuration | System | Events | SMTP Servers | Add' and the text 'Add an SMTP server.' Below this is a text input field labeled 'SMTP Server' with a placeholder 'Enter the IP address or hostname of the SMTP server.' and two buttons: 'Add' and 'Cancel'.

SMTP Server

Enter the IP address or hostname of the SMTP server. (If you have configured a DNS server, you can enter a hostname; otherwise, enter an IP address.)

Add or Apply / Cancel

To add this server to the list of SMTP servers, click **Add**. Or to apply your changes to this SMTP server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | SMTP Servers** screen. Any new server appears in the **SMTP Servers** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entry, click **Cancel**. The Manager returns to the **Configuration | System | Events | SMTP Servers** screen, and the **SMTP Servers** list is unchanged.

Configuration | System | Events | Email Recipients

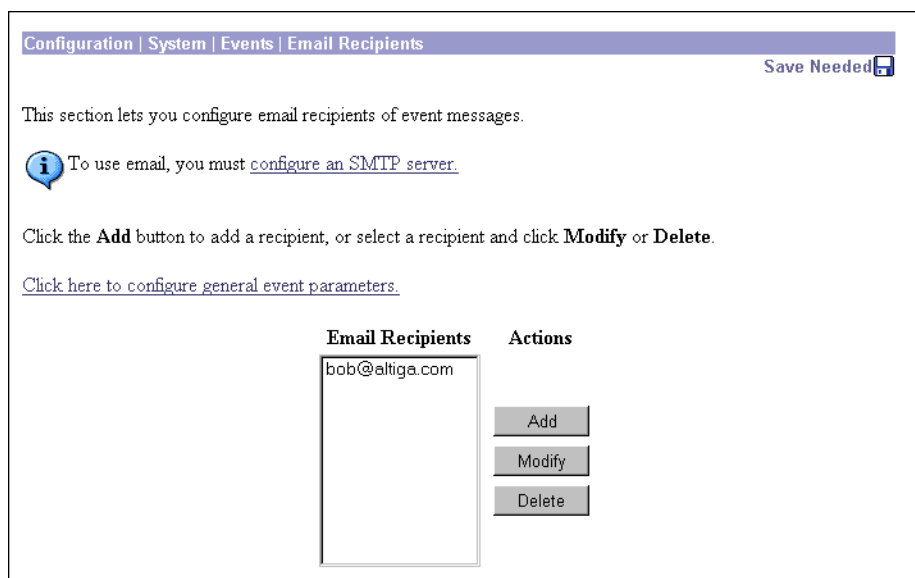
This section of the Manager lets you configure email recipients of event messages. You can configure a maximum of five email recipients, and you can customize the event message severity levels for each recipient.

If you configure any event handling—default or special—with values in **Severity to Email** fields, you must name at least one email recipient to receive the event messages, and you must identify at least one SMTP server to handle the outgoing email. You should also configure the **Email Source Address** on the **Configuration | System | Events | General** screen.

To configure SMTP servers, see the **Configuration | System | Events | SMTP Servers** screen, or click the highlighted link that says “*configure an SMTP server.*”

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the **Configuration | System | Events | Classes** screens.

Figure 10-12: Configuration | System | Events | Email Recipients screen



Email Recipients

The **Email Recipients** list shows configured event message email recipients in the order they were configured. You can configure a maximum of five email recipients. If no email recipients have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new email recipient, click **Add**. See **Configuration | System | Events | Email Recipients | Add**.

To modify an email recipient who has been configured, select the recipient from the list and click **Modify**. See **Configuration | System | Events | Email Recipients | Modify**.

To remove an email recipient who has been configured, select the recipient from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining recipients in the **Email Recipients** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Email Recipients | Add or Modify

These screens let you:

Add and configure an event message email recipient. You can configure a maximum of five email recipients.

Modify the parameters for a configured email recipient.

Figure 10-13: Configuration | System | Events | Email Recipients | Add or Modify screen

The screenshot shows two overlapping window titles. The top window is titled "Configuration | System | Events | Email Recipients | Modify" and contains the text "Modify a configured email recipient." The bottom window is titled "Configuration | System | Events | Email Recipients | Add" and contains the text "Add an email recipient." Below this text are two fields: "Email Address" with a text input box and a help text "Enter the recipient's complete email address (e.g. bob@company.com).", and "Max Severity" with a dropdown menu showing "1-3" and a help text "Select the maximum event severity this recipient is to receive." At the bottom of the "Add" window are two buttons: "Add" and "Cancel".

Email Address

Enter the recipient's complete email address; e.g., bob@altiga.com.

Max Severity

Click the drop-down menu button and select the range of event severity levels to send to this recipient via email. Choices are: **None**, **1**, **1-2**, **1-3**. The default is **1-3**: configured events of severity level 1 through severity level 3 are sent to this recipient.

The event levels emailed to this recipient are the *lesser of* the **Severity to Email** setting for a customized event class, or this **Max Severity** setting. If an event class has not been customized, the events emailed are the *lesser of* this setting or the default **Severity to Email** setting. For example, if you configure IPSEC events with severity levels 1-3 to email, all other events with no severity to email, and bob@altiga.com to receive email events of severity levels 1-2, bob will receive only IPSEC events of severity levels 1-2.

Add or Apply / Cancel

To add this recipient to the list of email recipients, click **Add**. Or to apply your changes to this email recipient, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | System | Events | Email Recipients** screen. Any new recipient appears at the bottom of the **Email Recipients** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entry, click **Cancel**. The Manager returns to the **Configuration | System | Events | Email Recipients** screen, and the **Email Recipients** list is unchanged.

End of Chapter



General

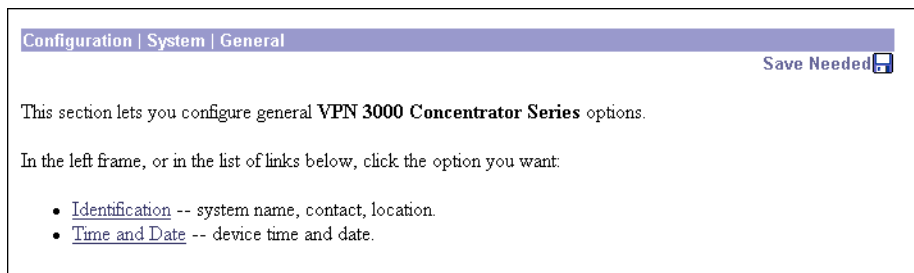
General configuration parameters include VPN 3000 Concentrator environment items: system identification, time, and date.

Configuration | System | General

This section of the Manager lets you configure general VPN Concentrator parameters.

- **Identification:** system name, contact person, system location.
- **Time and Date:** system time and date.

Figure 11-1: Configuration | System | General screen



Configuration | System | General | Identification

This screen lets you configure system identification parameters that are stored in the standard MIB-II system object. Network management systems using SNMP can retrieve this object and identify the system. Configuring this information is optional.

Figure 11-2: Configuration | System | General | Identification screen

Configuration | System | General | Identification

Configure system identification (optional). These entries are stored in the MIB-II system object.

System Name Enter a system name for the device; e.g., vpn01

Contact Enter the name of the contact person

Location Enter the device location; e.g., Computer Lab 3

System Name

Enter a system name that uniquely identifies this VPN Concentrator on your network; e.g., VPN01. Maximum 255 characters.

Contact

Enter the name of the contact person who is responsible for this VPN Concentrator. Maximum 255 characters.

Location

Enter the location of this VPN Concentrator. Maximum 255 characters.

Apply / Cancel

To apply your system identification settings and include them in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | General** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | General** screen.

Configuration | System | General | Time and Date

This screen lets you set the time and date on the VPN Concentrator. Setting the correct time is very important so that logging and accounting information is accurate.

Figure 11-3: Configuration | System | General | Time and Date screen

Current Time

The screen shows the current date and time on the VPN Concentrator at the time the screen displays. You can refresh this by redisplaying the screen.

New Time

The values in the **New Time** fields are the time and date on the *browser PC* at the time the screen displays. Any entries you make apply to the *VPN Concentrator*, however.

In the appropriate fields, make any changes. The fields are, in order: **Hour : Minute : Second AM/PM Month / Day / Year Time Zone**. Click the drop-down menu buttons to select **AM/PM**, **Month**, and **Time Zone**. The time zone selections are offsets in hours relative to GMT (Greenwich Mean Time), which is the basis for Internet time synchronization. Enter the **Year** as a four-digit number.

Enable DST Support

To enable DST support, check the box. During DST (Daylight-Saving Time), clocks are set one hour ahead of standard time. Enabling DST support means that the VPN Concentrator automatically adjusts the time zone for DST or standard time. *If your system is in a time zone that uses DST, you must enable DST support.*

Apply / Cancel

To apply your time and date settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the **Configuration | System | General** screen.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | System | General** screen.

End of Chapter



User Management

Groups and users are core concepts in managing the security of VPNs and in configuring the VPN 3000 Concentrator. Groups and users have attributes, configured via parameters, that determine their access to and use of the VPN. *Users* are members of *groups*, and groups are members of the *base group*. This section of the VPN 3000 Concentrator Series Manager lets you configure those parameters.

Groups simplify system management. And to streamline the configuration task, the VPN Concentrator provides a base group that you configure first. The base-group parameters are those that are most likely to be common across all groups and users. As you configure a group, you can simply specify that it “inherit” parameters from the base group; and a user can also “inherit” parameters from a group. Thus you can quickly configure authentication for large numbers of users.

Of course, if you decide to grant identical rights to all VPN users, then you don’t need to configure specific groups. But VPNs are seldom managed that way. For example, you might allow a Finance group to access one part of a private network, a Customer Support group to access another part, and an MIS group to access other parts. Further, you might allow specific users within MIS to access systems that other MIS users cannot access.

You can configure detailed parameters for groups and users on the VPN Concentrator internal authentication server. External RADIUS authentication servers also can return group and user parameters that match those on the VPN Concentrator; other authentication servers do not. The Cisco software CD-ROM includes a 30-day evaluation copy of Funk Software’s Steel-Belted RADIUS authentication server and instructions for using it with the VPN Concentrator.

You can configure a maximum of 100 groups and users (combined) in the VPN Concentrator internal server, which is adequate for a small user base. For larger numbers of users, we recommend using the internal server to configure groups (and perhaps a few users); and using a RADIUS server to authenticate the users.

The VPN Concentrator checks authentication parameters in this order:

- **First:** User parameters. If any parameters are missing, the system looks at:
- **Second:** Group parameters. If any parameters are missing, the system looks at:
- **(Third, for IPSec users only:** IPSec tunnel-group parameters. These are the parameters of the IPSec group used to create the tunnel. The IPSec group is configured on the internal server.) If any parameters are missing, the system looks at:
- **Last:** Base-group parameters.

If you use a non-RADIUS server, only the IPSec tunnel-group or base-group parameters apply to users.

Some additional points to note:

- Base-group parameters are the default, or system-wide, parameters.
- A user can be a member of only one group.
- Users who are not members of a specific group are, by default, members of the base group. Therefore, to ensure maximum security and control, you should assign all users to appropriate groups, and you should configure base-group parameters carefully.
- You can change group parameters, thereby changing parameters for all its members at the same time.
- You can delete a group, but when you do, all its members revert to the base group. Deleting a group, however, does not delete its members' user profiles.
- You can override the base-group parameters when you configure groups and users, and give groups and users more or fewer rights with this exception:
 - For PPTP and L2TP authentication protocols, you can allow specific groups and users to use *fewer* protocols than the base group, but not more.

For all other parameters, groups' and users' rights can be greater than the base group. For example, you can give a specific user 24-hour access to the VPN, but give the base group access during business hours only.

- To use both IPsec and L2TP over IPsec protocols for remote access, a user must be assigned to different groups, since the IPsec parameters differ.
- You apply filters to groups and users, and thus govern *tunneled* data traffic through the VPN Concentrator. You also apply filters to network interfaces, and thus govern *all* data traffic through the VPN Concentrator. See the **Configuration | Policy Management | Traffic Management** screens.
- We can supply a “dictionary” of Cisco-specific user and group parameters for external RADIUS servers.

We recommend that you *define* groups when planning your VPN, and that you *configure* groups and users on the VPN Concentrator in this order:

- Base-group parameters.
- Group parameters.
- User parameters.

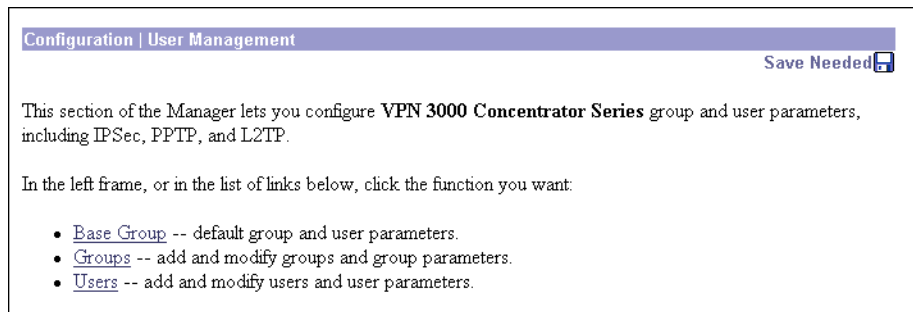
Before configuring groups and users, you should configure:

- System policies: network lists, access hours, filters, rules, and IPsec security associations (see **Configuration | Policy Management**).
- Authentication servers, and specifically the internal authentication server (see **Configuration | System | Servers**).

Configuration | User Management

This section of the Manager lets you configure base-group, group, and individual user parameters. These parameters determine access and use of the VPN Concentrator.

Figure 12-1: Configuration | User Management screen



Configuration | User Management | Base Group

This Manager screen lets you configure the default, or base-group, parameters. Base-group parameters are those that are most likely to be common across all groups and users, and they streamline the configuration task. Groups can “inherit” parameters from this base group, and users can “inherit” parameters from their group or the base group. You can override these parameters as you configure groups and users. Users who are not members of a group are, by default, members of the base group.

On this screen, you configure three kinds of parameters:

- **General Parameters:** security, access, performance, and protocols.
- **IPSec Parameters:** IP Security tunneling protocol.
- **PPTP/L2TP Parameters:** PPTP and L2TP tunneling protocols.

Before configuring these parameters, you should configure:

- Access Hours (**Configuration | Policy Management | Access Hours**).
- Rules and filters (**Configuration | Policy Management | Traffic Management | Rules and Filters**).
- IPSec Security Associations (**Configuration | Policy Management | Traffic Management | Security Associations**).
- Network Lists for filtering and split tunneling (**Configuration | Policy Management | Traffic Management | Network Lists**).
- User Authentication servers, and specifically the internal authentication server (**Configuration | System | Servers | Authentication**).

Using the tabs

This screen includes three tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Apply** or **Cancel**.

Figure 12-2: Configuration | User Management | Base Group screen, General tab

Configuration | User Management | Base Group

General
IPSec
PPTP/L2TP

General Parameters		
Attribute	Value	Description
Access Hours	<input type="text" value="-No Restrictions-"/>	Select the access hours for this group.
Simultaneous Logins	<input type="text" value="3"/>	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	<input type="text" value="8"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Check to allow alphabetic-only passwords for users in this group.
Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	Select the tunneling protocols this group can connect with.

Apply
Cancel

General Parameters tab

This tab lets you configure general security, access, performance, and protocol parameters that apply to the base group.

Access Hours

Click the drop-down menu button and select the named hours when remote-access users can access the VPN Concentrator. Configure access hours on the **Configuration | Policy Management | Access Hours** screen. Default entries are:

-No Restrictions- = No named access hours applied (the default), which means that there are no restrictions on access hours.

Never = No access at any time.

Business Hours = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for a single user. The minimum is 0, which disables login and prevents user access; default is 3. While there is no maximum limit, allowing several could compromise security and affect performance.

Minimum Password Length

Enter the minimum number of characters for user passwords. The minimum is 1, the default is 8, and the maximum is 32. To protect security, we strongly recommend 8 or higher.

Allow Alphabetic-Only Passwords

Check the box to allow user passwords with alphabetic characters only (the default). This option applies only to users who are configured in and authenticated by the VPN Concentrator internal authentication server. To protect security, we strongly recommend that you *not* allow such passwords; i.e., that you require passwords to be a mix of alphabetic characters, numbers, and symbols, such as 648e&9G#.

Idle Timeout

Enter the idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1, the default is 30 minutes, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Maximum Connect Time

Enter the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter 0 (the default).

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the **Configuration | Policy Management | Traffic Management** screens.

Click the drop-down menu button and select the base-group filter:

--None-- = No filter applied, which means there are no restrictions on tunneled data traffic. This is the default selection.

Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)

Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)

External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

Primary DNS

Enter the IP address, in dotted decimal notation, of the primary DNS server for base-group users. The system sends this address to the client as the first DNS server to use for resolving hostnames. If the base group doesn't use DNS, leave this field blank. See the *Note on DNS and WINS entries* under **Configuration | User Management | Groups | Add** on page 12-22.

Secondary DNS

Enter the IP address, in dotted decimal notation, of the secondary DNS server for base-group users. The system sends this address to the client as the second DNS server to use for resolving hostnames.

Primary WINS

Enter the IP address, in dotted decimal notation, of the primary WINS server for base-group users. The system sends this address to the client as the first WINS server to use for resolving hostnames under Windows NT. If the base group doesn't use WINS, leave this field blank. See the *Note on DNS and WINS entries* under **Configuration | User Management | Groups | Add** on page 12-22.

Secondary WINS

Enter the IP address, in dotted decimal notation, of the secondary WINS server for base-group users. The system sends this address to the client as the second WINS server to use for resolving hostnames under Windows NT.

SEP Card Assignment

The VPN Concentrator can contain up to four SEP (Scalable Encryption Processing) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle up to 5000 sessions (users)—the system maximum. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the box to assign the load to a given SEP module. By default, all boxes are checked, and we recommend you keep the default. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired boxes to select the VPN tunneling protocols that user clients can use. Configure parameters on the **IPSec** or **PPTP/L2TP** tabs as appropriate. Clients can use only the selected protocols.

You cannot check both **IPSec** and **L2TP over IPSec**. The IPSec parameters differ for these two protocols, and you cannot configure the base group for both.

PPTP = Point-to-Point Tunneling Protocol (checked by default). PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000.

L2TP = Layer 2 Tunneling Protocol (checked by default). L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).

IPSec = IP Security Protocol (checked by default). IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec. The Cisco VPN 3000 Client is an IPSec

client specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients.

L2TP over IPSec = L2TP using IPSec for security (not checked by default). L2TP packets are encapsulated within IPSec, thus providing an additional authentication and encryption layer for security. L2TP over IPSec is a client-server protocol, and it provides interoperability with the Windows 2000 VPN client and other compliant remote-access clients.

Note: If no protocol is selected, no user clients can access or use the VPN.

Figure 12-3: Configuration | User Management | Base Group screen, IPSec tab

Configuration User Management Base Group		
General IPSec PPTP/L2TP		
IPSec Parameters		
Attribute	Value	Description
IPSec SA	ESP-3DES-MD5	Select the IPSec Security Association assigned to this group.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	Lock the users into this group.
Authentication	Internal	Select the authentication method for users in this group.
Mode Configuration	<input checked="" type="checkbox"/>	Check to use Mode Configuration for users of this group. Update parameters below if checked.
Mode Configuration Parameters		
Banner		Enter the banner for this group.
Allow Password Storage on Client	<input type="checkbox"/>	Check to allow the IPSec client to store the password locally.
Split Tunneling Network List	-None-	Select the Network List to be used for Split Tunneling.
Default Domain Name		Enter the default domain name given to users of this group.
IPSec through NAT	<input type="checkbox"/>	Check to allow the IPSec client to operate through a firewall using NAT via UDP.
IPSec through NAT UDP Port	10000	Enter the UDP port to be used for IPSec through NAT (4001 - 49151).
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

IPSec Parameters tab

This tab lets you configure IP Security Protocol parameters that apply to the base group. If you checked **IPSec** or **L2TP over IPSec** under **Tunneling Protocols** on the **General Parameters** tab, configure this section.

IPSec SA

Click the drop-down menu button and select the IPSec Security Association (SA) assigned to IPSec clients. During tunnel establishment, the client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the **Configuration | Policy Management | Traffic Management | Security Associations** screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screens.

The VPN Concentrator supplies these default selections:

--None-- = No SA assigned. Select this option if you need to configure groups with several different SAs.

ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel. This is the default selection.

ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the **L2TP over IPSec** tunneling protocol.

Additional SAs that you have configured also appear on the list.

Tunnel Type

Click the drop-down menu button and select the type of IPSec tunnel that clients use:

LAN-to-LAN = IPSec LAN-to-LAN connections between two VPN Concentrators (or between a VPN Concentrator and another protocol-compliant security gateway). See **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN**. If you select this type, ignore the rest of the parameters on this tab.

Remote Access = Remote IPSec client connections to the VPN Concentrator (the default). If you select this type, configure **Remote Access Parameters** below.

Remote Access Parameters

These base-group parameters apply to remote-access IPSec client connections only. If you select **Remote Access** for **Tunnel Type**, configure these parameters.

Group Lock

Check the box to restrict users to remote access through this group only. The IPSec client connects to the VPN Concentrator via a group name and password, and then the system authenticates a user via a username and password. If this box is not checked (the default), the system authenticates a user without regard to the user's assigned group.

Authentication

Click the drop-down menu button and select the user authentication method (authentication server type) to use with remote-access IPsec clients. This selection identifies the authentication *method*, not the specific server. Configure authentication servers on the **Configuration | System | Servers | Authentication** screens.

Selecting any authentication method (other than **None**) enables ISAKMP Extended Authentication, also known as XAuth.

None = No IPsec user authentication method. If you checked **L2TP over IPsec** under **Tunneling Protocols**, use this selection.

RADIUS = Authenticate users via external Remote Authentication Dial-In User Service.

NT Domain = Authenticate users via external Windows NT Domain system.

SDI = Authenticate users via external RSA Security Inc. SecureID system.

Internal = Authenticate users via the internal VPN Concentrator authentication server. This is the default selection.

Mode Configuration

Check the box to use Mode Configuration with IPsec clients (also known as the ISAKMP Configuration Method or Configuration Transaction). This option exchanges configuration parameters with the client while negotiating Security Associations. If you check this box, configure the desired **Mode Configuration Parameters** below; otherwise, ignore them. The box is checked by default.

To use split tunneling, you must check this box.

If you checked **L2TP over IPsec** under **Tunneling Protocols**, *do not* check this box.

Notes: *IPsec uses Mode Configuration to pass **all** configuration parameters to a client: IP address, DNS and WINS addresses, etc. You **must** check this box to use Mode Configuration. Otherwise, those parameters—even if configured with entries—are not passed to the client.*

The Cisco VPN 3000 Client (IPsec client) supports Mode Configuration, but other IPsec clients may not. For example, the Microsoft Windows 2000 IPsec client does *not* support Mode Configuration. (The Windows 2000 client uses the PPP layer above L2TP to receive its IP address from the VPN Concentrator.) Determine compatibility before using this option with other vendors' clients.

Mode Configuration Parameters

These base-group parameters apply to IPsec clients using Mode Configuration. If you check **Mode Configuration** above, configure these parameters as desired; otherwise, ignore them.

Banner

Enter the banner, or text string, that remote-access IPsec clients see when they log in. The maximum length is 128 characters.

Allow Password Storage on Client

Check the box to allow IPSec clients to store their login passwords on their local client systems. If you do not allow password storage (the default), IPSec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

Split Tunneling Network List

Click the drop-down menu button and select the Network List to use for split tunneling. If no Network Lists have been configured, the list shows **--None--**, which means that split tunneling is disabled (the default). Selecting a configured Network List enables split tunneling. Configure Network Lists on the **Configuration | Policy Management | Traffic Management | Network Lists** screens.

We recommend that you keep the base-group default, and that you enable and configure split tunneling selectively for each group.

You can apply only one Network List to a group, but one Network List can contain up to 200 network entries.

About split tunneling and Network Lists

Split tunneling lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. Packets not bound for destinations across the IPSec tunnel don't have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination. Split tunneling thus eases the processing load, simplifies traffic management, and speeds up untunneled traffic.

Split tunneling applies only to single-user remote-access IPSec tunnels, not to LAN-to-LAN connections.

Split tunneling decisions depend on the destination network address; hence the use of Network Lists. A Network List is a list of addresses on the private network. The IPSec client uses the Network List as an *inclusion* list: a list of networks for which traffic should be sent over the IPSec tunnel. All other traffic is routed as normal cleartext traffic.

The IPSec client establishes an IPSec Security Association (SA) for each network specified in the list. Outbound packets with destination addresses that match one of the SAs are sent over the tunnel; everything else is sent as clear text to the locally connected network.

Split tunneling can act as a packet filter at the client. If a Network List defines only a subset of the private network address space, then a client can access only that subset of network addresses. The client cannot access other addresses because packets to those addresses are sent to the public Internet, from which they are not accessible.

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you *not* enable split tunneling. However, since only the VPN Concentrator—and not the IPSec client—can enable split tunneling, you can control implementation here and thus protect security. Split tunneling is disabled by default on both the VPN Concentrator and the client. You enable and configure the feature here, and then the VPN Concentrator uses Mode Configuration to push it to, and enable it on, the IPSec client.

You must create a Network List before you can enable split tunneling. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens.

Default Domain Name

Enter the default domain name that the VPN Concentrator passes to the IPsec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. For example, if this entry is `xyzcorp.com`, a DNS query for `mail` becomes `mail.xyzcorp.com`. Maximum is 255 characters. The Manager checks the domain name for valid syntax.

IPsec through NAT

Check the box to allow the Cisco VPN 3000 Client (IPsec client) to connect to the VPN Concentrator via UDP through a firewall or router using NAT. The box is not checked by default. See discussion below.

IPsec through NAT UDP Port

Enter the UDP port number to use if you allow **IPsec through NAT**. Enter a number in the range 4001 through 49151; default is 10000.

About IPsec through NAT

IPsec through NAT lets you use the Cisco VPN 3000 Client to connect to the VPN Concentrator via UDP through a firewall or router that is running NAT. This feature is proprietary, it applies only to remote-access connections, and it requires Mode Configuration. Using this feature may slightly degrade system performance.

Enabling this feature creates runtime filter rules that forward UDP traffic for the configured port even if other filter rules on the interface drop UDP traffic. These runtime rules exist only while there is an active IPsec through NAT session. The system passes inbound traffic to IPsec for decryption and unencapsulation, and then passes it to the destination. The system passes outbound traffic to IPsec for encryption and encapsulation, applies a UDP header, and forwards it.

You can configure more than one group with this feature enabled, and each group can use a different port number. Port numbers must be in the 4001 through 49151 range, which is a subset of the IANA Registered Ports range.

The Cisco VPN 3000 Client must also be configured to use this feature (it is configured to use it by default). The VPN Client Connection Status dialog box indicates if the feature is being used. See the *VPN 3000 Client User Guide*.

The **Administration | Sessions** and **Monitor | Sessions** screens indicate if a session is using IPsec through NAT, and the **Detail** screens show the UDP port.

Figure 12-4: Configuration | User Management | Base Group screen, PPTP/L2TP tab

Configuration User Management Base Group		
PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

Apply Cancel

PPTP/L2TP Parameters tab

This tab lets you configure PPTP and L2TP parameters that apply to the base group. During tunnel establishment, the client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked **PPTP**, **L2TP**, or **L2TP over IPsec** under **Tunneling Protocols** on the **General Parameters** tab, configure these parameters.

Use Client Address

Check the box to accept and use an IP address that the client supplies. A client must have an IP address to function as a tunnel endpoint; but for maximum security, we recommend that you control IP address assignment and *not allow* client-supplied IP addresses (the default).

Make sure the setting here is consistent with the setting for **Use Client Address** on the **Configuration | System | Address Management | Assignment** screen.

PPTP Authentication Protocols

Check the boxes for the authentication protocols that PPTP clients can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol (the default).

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, and is allowed by default.

EAP = Extensible Authentication Protocol. This protocol is allowed by default. It supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). This protocol is allowed by default. If you check **Required** under **PPTP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. This protocol is not allowed by default. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check **Required** under **PPTP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

PPTP Encryption

Check the boxes for the data encryption options that apply to PPTP clients.

Required = During connection setup, PPTP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. This option is not checked by default. If you check this option, you must also allow only **MSCHAPv1** and/or **MSCHAPv2** under **PPTP Authentication Protocols** above, and you must also check **40-bit** and/or **128-bit** here. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.

Require Stateless = During connection setup, PPTP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet. This option is not checked by default. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.

40-bit = PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the **128-bit** option. Microsoft encryption (MPPE) uses this algorithm. This option is checked by default. If you check **Required**, you must check this option and/or the **128-bit** option.

128-bit = PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. This option is checked by default. If you check **Required**, you must check this option and/or the **40-bit** option. The U.S. government restricts the distribution of 128-bit encryption software.

L2TP Authentication Protocols

Check the boxes for the authentication protocols that L2TP clients can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol (the default).

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP, and is allowed by default.

EAP = Extensible Authentication Protocol. This protocol is allowed by default. It supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). This protocol is allowed by default. If you check **Required** under **L2TP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. This protocol is not allowed by default. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check **Required** under **L2TP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

L2TP Encryption

Check the boxes for the data encryption options that apply to L2TP clients.

Required = During connection setup, L2TP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. This option is not checked by default. If you check this option, you must also allow only **MSCHAPv1** and/or **MSCHAPv2** under **L2TP Authentication Protocols** above, and you must also check **40-bit** and/or **128-bit** here. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.

Require Stateless = During connection setup, L2TP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet. This option is not checked by default. Do not check this option if you use NT Domain user authentication; NT Domain authentication cannot negotiate encryption.

40-bit = L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the **128-bit** option. Microsoft encryption (MPPE) uses this algorithm. This option is not checked by default. If you check **Required**, you must check this option and/or the **128-bit** option.

128-bit = L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. This option is not checked by default. If you check **Required**, you must check this option and/or the **40-bit** option. The U.S. government restricts the distribution of 128-bit encryption software.

Apply / Cancel

When you finish setting base-group parameters on all tabs, click **Apply** at the bottom of the screen to include your settings in the active configuration. The Manager returns to the **Configuration | User Management** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | User Management** screen.

Configuration | User Management | Groups

This section of the Manager lets you configure access and usage parameters for specific groups. A group is a collection of users treated as a single entity. Groups inherit parameters from the base group.

See the discussion of groups and users under *User Management* at the beginning of this chapter.

Configuring internal groups in this section means configuring them on the VPN Concentrator internal authentication server. If you have not configured the internal authentication server, this screen displays a notice that includes a link to the **Configuration | System | Servers | Authentication** screen. The system also automatically configures the internal server when you add the first internal group.

Configuring external groups means configuring them on an external authentication server such as RADIUS or NT Domain.

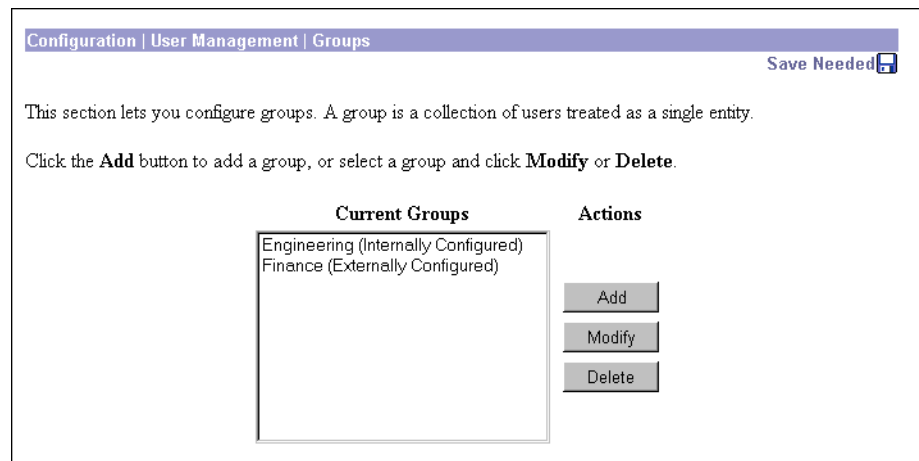
Note: If a RADIUS server is configured to return the Class attribute (#25), the VPN Concentrator uses that attribute to authenticate the **Group Name**. On the RADIUS server, the attribute must be formatted as:

```
OU=groupname;
```

where `groupname` is identical to the **Group Name** configured on the VPN Concentrator. For example,

```
OU=Finance;
```

Figure 12-5: Configuration | User Management | Groups screen



Current Groups

The **Current Groups** list shows configured groups in alphabetical order, and if they are internal or external. If no groups have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure and add a new group, click **Add**. The Manager opens the **Configuration | User Management | Groups | Add** screen.

To modify parameters for a group that has been configured, select the group from the list and click **Modify**. The Manager opens the appropriate internal or external **Configuration | User Management | Groups | Modify** screen.

To remove a group that has been configured, select the group from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining groups in the list. *When you delete a group, all its members revert to the base group.* Deleting a group, however, does not delete its members' user profiles.

You cannot delete a group that is configured as part of a LAN-to-LAN connection. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | User Management | Groups | Add or Modify (Internal)

These screens let you:

Add: Configure and add a new group.

Modify: Change parameters for a group that you have previously configured on the internal server. The screen title identifies the group you are modifying.

For many of these parameters, you can simply specify that the group “inherit” parameters from the base group, which you should configure first. You can also override the base-group parameters as you configure groups. See the **Configuration | User Management | Base Group** screen.

On this screen, you configure four kinds of parameters:

- **Identity Parameters:** name, password, and type.
- **General Parameters:** security, access, performance, and protocols.
- **IPSec Parameters:** IP Security tunneling protocol.
- **PPTP/L2TP Parameters:** PPTP and L2TP tunneling protocols.

Using the tabs

This screen includes four tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Add / Apply** or **Cancel**.

Figure 12-6: Configuration | User Management | Groups | Add or Modify (Internal) screen, Identity tab

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text"/>	Enter a unique name for the group.
Password	<input type="text"/>	Enter the password for the group.
Verify	<input type="text"/>	Verify the group's password.
Type	Internal <input type="button" value="v"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator Series's Internal Database.

Add Cancel

Identity Parameters tab

This tab lets you configure the name, password, and authentication server type for this group.

Group Name

Enter a unique name for this specific group. Maximum is 32 characters, case-sensitive. Changing a group name automatically updates the group name for all users in the group.

See the note about configuring the RADIUS Class attribute under **Configuration | User Management | Groups** on page 12-16.

Password

Enter a unique password for this group. Minimum is 4, maximum is 32 characters, case-sensitive. The field displays only asterisks.

Verify

Re-enter the group password to verify it. The field displays only asterisks.

Type

Click the drop-down menu button and select the authentication server type (authentication method) for this group:

Internal = Use the internal VPN Concentrator authentication server. This is the default selection. If you select this type, configure the parameters on the other tabs on this screen. The VPN Concentrator automatically configures its internal server when you add the first internal group.

External = Use an external authentication server—such as RADIUS—for this group. If you select this type, *ignore the rest of the tabs and parameters on this screen*. The external server supplies the group parameters if it can; otherwise the base-group parameters apply.

Figure 12-7: Configuration | User Management | Groups | Add or Modify (Internal) screen, General tab

Monitoring | User Management | Groups | Modify Engineering

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this group can connect with.

Add Cancel

General Parameters tab

This tab lets you configure general security, access, performance, and tunneling protocol parameters that apply to this internally configured group.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group

setting, clear the check box. If you clear the check box, you must also enter or change any corresponding **Value** field; do not leave the field blank.

- The **Value** column thus shows either base-group parameter settings that also apply to this group (**Inherit?** checked), or unique parameter settings configured for this group (**Inherit?** cleared).

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Access Hours

Click the drop-down menu button and select the named hours when this group's remote-access users can access the VPN Concentrator. Configure access hours on the **Configuration | Policy Management | Access Hours** screen. Default entries are:

-No Restrictions- = No named access hours applied, which means that there are no restrictions on access hours.

Never = No access at any time.

Business Hours = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for a single user in this group. The minimum is 0, which disables login and prevents user access. While there is no maximum limit, allowing several could compromise security and affect performance.

Minimum Password Length

Enter the minimum number of characters for this group's user passwords. The minimum is 1, and the maximum is 32. To protect security, we strongly recommend 8 or higher.

Allow Alphabetic-Only Passwords

Check the box to allow this group's user passwords with alphabetic characters only. This option applies only to users who are configured in and authenticated by the VPN Concentrator internal authentication server. To protect security, we strongly recommend that you *not* allow such passwords; i.e., that you require passwords to be a mix of alphabetic characters, numbers, and symbols, such as 648e&9G#.

Idle Timeout

Enter the group's idle timeout period in minutes. If there is no communication activity on a user connection in this period, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Maximum Connect Time

Enter the group's maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter 0.

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the **Configuration | Policy Management | Traffic Management** screens.

Click the drop-down menu button and select the filter to apply to this group's users:

--None-- = No filter applied, which means there are no restrictions on tunneled data traffic.

Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)

Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)

External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

Note on DNS and WINS entries below:

If the base group uses DNS or WINS, and:

— this group uses the base-group setting: check the appropriate **Inherit?** box (the default).

— this group uses different DNS or WINS servers: clear the appropriate **Inherit?** check box and enter this group's server IP address(es).

— this group doesn't use DNS or WINS: clear the appropriate **Inherit?** check box and enter 0.0.0.0 in the IP address field.

If the base group does not use DNS or WINS, and:

— this group also does not use DNS or WINS: check the appropriate **Inherit?** check box (the default).

— this group uses DNS or WINS: clear the appropriate **Inherit?** check box and enter this group's server IP address(es).

Primary DNS

Enter the IP address, in dotted decimal notation, of the primary DNS server for this group's users. The system sends this address to the client as the first DNS server to use for resolving hostnames. See note above.

Secondary DNS

Enter the IP address, in dotted decimal notation, of the secondary DNS server for this group's users. The system sends this address to the client as the second DNS server to use for resolving hostnames. See note above.

Primary WINS

Enter the IP address, in dotted decimal notation, of the primary WINS server for this group's users. The system sends this address to the client as the first WINS server to use for resolving hostnames under Windows NT. See note above.

Secondary WINS

Enter the IP address, in dotted decimal notation, of the secondary WINS server for this group's users. The system sends this address to the client as the second WINS server to use for resolving hostnames under Windows NT. See note above.

SEP Card Assignment

The VPN Concentrator can contain up to four SEP (Scalable Encryption Processing) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle up to 5000 sessions (users)—the system maximum. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the box to assign this group's load to a given SEP module. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired boxes to select the VPN tunneling protocols that this group's user clients can use. Configure parameters on the **IPSec** or **PPTP/L2TP** tabs as appropriate. Clients can use only the selected protocols.

You cannot check both **IPSec** and **L2TP over IPSec**. The IPSec parameters differ for these two protocols, and you cannot configure a single group for both.

PPTP = Point-to-Point Tunneling Protocol. PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000.

L2TP = Layer 2 Tunneling Protocol. L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).

IPSec = IP Security Protocol. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec. The Cisco VPN 3000 Client is an IPSec client specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients.

L2TP over IPSec = L2TP using IPSec for security. L2TP packets are encapsulated within IPSec, thus providing an additional authentication and encryption layer for security. L2TP over IPSec is a client-server protocol, and it provides interoperability with the Windows 2000 VPN client and other compliant remote-access clients.

Note: If no protocol is selected, none of this group's user clients can access or use the VPN.

Figure 12-8: Configuration | User Management | Groups | Add or Modify (Internal) screen, IPSec tab

Monitoring | User Management | Groups | Modify Engineering

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for users in this group.
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use Mode Configuration for users of this group. Update parameters below if checked.
Mode Configuration Parameters			
Banner		<input checked="" type="checkbox"/>	Enter the banner for this group.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.
Split Tunneling Network List	-None-	<input checked="" type="checkbox"/>	Select the Network List to be used for Split Tunneling.
Default Domain Name		<input checked="" type="checkbox"/>	Enter the default domain name given to users of this group.
IPSec through NAT	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to operate through a firewall using NAT via UDP.
IPSec through NAT UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151).

Add Cancel

IPSec Parameters tab

This tab lets you configure IP Security Protocol parameters that apply to this internally configured group. If you checked **IPSec** or **L2TP over IPSec** under **Tunneling Protocols** on the **General Parameters** tab, configure this section.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, clear the check box. If you clear the check box, you must also enter or change any corresponding **Value** field; do not leave the field blank.
- The **Value** column thus shows either base-group parameter settings that also apply to this group (**Inherit?** checked), or unique parameter settings configured for this group (**Inherit?** cleared).

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

IPSec SA

Click the drop-down menu button and select the IPSec Security Association (SA) assigned to this group's IPSec clients. During tunnel establishment, the client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the **Configuration | Policy Management | Traffic Management | Security Associations** screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screens.

The VPN Concentrator supplies these default selections:

--None-- = No SA assigned.

ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.

ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the **L2TP over IPSec** tunneling protocol.

Additional SAs that you have configured also appear on the list.

Tunnel Type

Click the drop-down menu button and select the type of IPSec tunnel that this group's clients use:

LAN-to-LAN = IPSec LAN-to-LAN connections between two VPN Concentrators (or between a VPN Concentrator and another protocol-compliant security gateway). See **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN**. If you select this type, ignore the rest of the parameters on this tab.

Remote Access = Remote IPSec client connections to the VPN Concentrator. If you select this type, configure **Remote Access Parameters** below.

Remote Access Parameters

These group parameters apply to remote-access IPSec client connections only. If you select **Remote Access** for **Tunnel Type**, configure these parameters.

Group Lock

Check the box to restrict users to remote access through this group only. The IPSec client connects to the VPN Concentrator via a group name and password, and then the system authenticates a user via a username and password. If this box is not checked, the system authenticates a user without regard to the user's assigned group.

Authentication

Click the drop-down menu button and select the user authentication method (authentication server type) to use with this group's remote-access IPSec clients. This selection identifies the authentication *method*, not the specific server. Configure authentication servers on the **Configuration | System | Servers | Authentication** screens.

Selecting any authentication method (other than **None**) enables ISAKMP Extended Authentication, also known as XAuth.

None = No IPSec user authentication method. If you checked **L2TP over IPSec** under **Tunneling Protocols**, use this selection.

RADIUS = Authenticate users via external Remote Authentication Dial-In User Service.

NT Domain = Authenticate users via external Windows NT Domain system.

SDI = Authenticate users via external RSA Security Inc. SecureID system.

Internal = Authenticate users via internal VPN Concentrator authentication server.

Mode Configuration

Check the box to use Mode Configuration with this group's IPSec clients (also known as the ISAKMP Configuration Method or Configuration Transaction). This option exchanges configuration parameters with the client while negotiating Security Associations. If you check this box, configure the desired **Mode Configuration Parameters** below; otherwise, ignore them.

To use split tunneling, you must check this box.

If you checked **L2TP over IPSec** under **Tunneling Protocols**, *do not* check this box.

Notes: *IPSec uses Mode Configuration to pass **all** configuration parameters to a client: IP address, DNS and WINS addresses, etc. You **must** check this box to use Mode Configuration. Otherwise, those parameters—even if configured with entries—are not passed to the client.*

The Cisco VPN 3000 Client (IPSec client) supports Mode Configuration, but other IPSec clients may not. For example, the Microsoft Windows 2000 IPSec client does *not* support Mode Configuration. (The Windows 2000 client uses the PPP layer above L2TP to receive its IP address from the VPN Concentrator.) Determine compatibility before using this option with other vendors' clients.

Mode Configuration Parameters

These parameters apply to this group's IPSec clients using Mode Configuration. If you check **Mode Configuration** above, configure these parameters as desired; otherwise, ignore them.

Banner

Enter the banner, or text string, that this group's IPSec clients see when they log in. The maximum length is 128 characters.

Allow Password Storage on Client

Check the box to allow this group's IPSec clients to store their login passwords on their local client systems. If you do not allow password storage, IPSec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

Split Tunneling Network List

Click the drop-down menu button and select the Network List to use for split tunneling. If no Network Lists have been configured, the list shows **--None--**, which means that split tunneling is disabled. Selecting a configured Network List enables split tunneling. Configure Network Lists on the **Configuration | Policy Management | Traffic Management | Network Lists** screens.

See the discussion *About split tunneling and Network Lists* under **Configuration | User Management | Base Group** on page 12-10.

You can apply only one Network List to a group, but one Network List can contain up to 200 network entries.

Default Domain Name

Enter the default domain name that the VPN Concentrator passes to the IPSec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. For example, if this entry is `xyzcorp.com`, a DNS query for `mail` becomes `mail.xyzcorp.com`. Maximum is 255 characters. The Manager checks the domain name for valid syntax.

IPSec through NAT

Check the box to allow the Cisco VPN 3000 Client (IPSec client) to connect to the VPN Concentrator via UDP through a firewall or router using NAT.

IPSec through NAT UDP Port

Enter the UDP port number to use if you allow **IPSec through NAT**. Enter a number in the range 4001 through 49151; default is 10000.

See the discussion *About IPSec through NAT* under **Configuration | User Management | Base Group** on page 12-11.

Figure 12-9: Configuration | User Management | Groups | Add or Modify (Internal) screen, PPTP/L2TP tab

Monitoring | User Management | Groups | Modify Engineering

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] ▼ <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Select the authentication protocols this group is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] ▼ <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Select the authentication protocols this group is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for L2TP connections for this group.

PPTP/L2TP Parameters tab

This section of the screen lets you configure PPTP and L2TP parameters that apply to this internally configured group. During tunnel establishment, the client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked **PPTP**, **L2TP**, or **L2TP over IPSec** under **Tunneling Protocols** on the **General Parameters** tab, configure these parameters.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to base-group parameters: Does this specific group inherit the given setting from the base group? To inherit the setting, check the box (default). To override the base-group setting, clear the check box. If you clear the check box, you must also enter or change any corresponding **Value** field; do not leave the field blank.
- The **Value** column thus shows either base-group parameter settings that also apply to this group (**Inherit?** checked), or unique parameter settings configured for this group (**Inherit?** cleared).

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Use Client Address

Check the box to accept and use an IP address that this group's client supplies. A client must have an IP address to function as a tunnel endpoint; but for maximum security, we recommend that you control IP address assignment and *not allow* client-specified IP addresses.

Make sure the setting here is consistent with the setting for **Use Client Address** on the **Configuration | System | Address Management | Assignment** screen.

PPTP Authentication Protocols

Check the boxes for the authentication protocols that this group's PPTP clients can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure.

You can allow a group to use *fewer* protocols than the base group, but not more. You cannot allow a grayed-out protocol.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol.

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP.

EAP = Extensible Authentication Protocol. This protocol supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—

and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). If you check **Required** under **PPTP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check **Required** under **PPTP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

PPTP Encryption

Check the boxes for the data encryption options that apply to this group's PPTP clients.

Required = During connection setup, this group's PPTP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. If you check this option, you must also allow only **MSCHAPv1** and/or **MSCHAPv2** under **PPTP Authentication Protocols** above, and you must also check **40-bit** and/or **128-bit** here.

Require Stateless = During connection setup, this group's PPTP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet.

40-bit = This group's PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the **128-bit** option. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the **128-bit** option.

128-bit = This group's PPTP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the **40-bit** option. The U.S. government restricts the distribution of 128-bit encryption software.

L2TP Authentication Protocols

Check the boxes for the authentication protocols that this group's L2TP clients can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure. You can allow a group to use *fewer* protocols than the base group, but not more. You cannot allow a grayed-out protocol.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol.

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP.

EAP = Extensible Authentication Protocol. This protocol supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption). If you check **Required** under **L2TP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths. The VPN Concentrator internal user authentication server supports this protocol, but external authentication servers do not. If you check **Required** under **L2TP Encryption** below, you must allow one or both **MSCHAP** protocols and no other.

L2TP Encryption

Check the boxes for the data encryption options that apply to this group's L2TP clients.

Required = During connection setup, this group's L2TP clients must agree to use Microsoft encryption (MPPE) to encrypt data or they will not be connected. If you check this option, you must also allow only **MSCHAPv1** and/or **MSCHAPv2** under **L2TP Authentication Protocols** above, and you must also check **40-bit** and/or **128-bit** here.

Require Stateless = During connection setup, this group's L2TP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet; otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, it might perform better in a lossy environment (where packets are lost), such as the Internet.

40-bit = This group's L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 40-bit key. This is significantly less secure than the **128-bit** option. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the **128-bit** option.

128-bit = This group's L2TP clients are allowed to use the RSA RC4 encryption algorithm with a 128-bit key. Microsoft encryption (MPPE) uses this algorithm. If you check **Required**, you must check this option and/or the **40-bit** option. The U.S. government restricts the distribution of 128-bit encryption software.

Add or Apply / Cancel

When you finish setting or changing parameters on all tabs, click **Add** or **Apply** at the bottom of the screen to **Add** this specific group to the list of configured groups, or to **Apply** your changes. Both actions include your settings in the active configuration. The Manager returns to the **Configuration | User Management | Groups** screen. Any new groups appear in alphabetical order in the **Current Groups** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click the **Cancel** button. The Manager returns to the **Configuration | User Management | Groups** screen, and the **Current Groups** list is unchanged.

Configuration | User Management | Groups | Modify (External)

This screen lets you change identity parameters for an external group that you have previously configured. The screen title identifies the group you are modifying.

Figure 12-10: Configuration | User Management | Groups | Modify (External) screen

Monitoring | User Management | Groups | Modify Finance

This section lets you modify an external group.

Identity

Identity Parameters		
Attribute	Value	Description
Group Name	Finance	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	External	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator Series's Internal Database.

Apply Cancel

Group Name

Enter a unique name for this specific group. You can edit this field as desired. Maximum is 32 characters, case-sensitive. Changing a group name automatically updates the group name for all users in the group.

See the note about configuring the RADIUS Class attribute under **Configuration | User Management | Groups** on page 12-16.

Password

Enter a unique password for this group. Minimum is 4, maximum is 32 characters, case-sensitive. The field displays only asterisks.

Verify

Re-enter the group password to verify it. The field displays only asterisks.

Type

Click the drop-down menu button and select the authentication server type for the group:

Internal = To change this group to use the internal VPN Concentrator authentication server, select this type. If you change this group from **External** to **Internal**, the Manager displays the **Configuration | User Management | Groups | Modify (Internal)** screen when you click **Apply**, so you can configure all the parameters.

External = To use only an external authentication server, such as RADIUS, keep this selection. The external server supplies the group parameters if it can; otherwise the base-group parameters apply.

Apply / Cancel

When you finish changing these parameters, click **Apply** to include your settings in the active configuration. The Manager returns to the **Configuration | User Management | Groups** screen and refreshes the **Current Groups** list. However, if you change group type to **Internal**, the Manager displays the **Configuration | User Management | Groups | Modify (Internal)** screen so you can configure all the parameters.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your changes, click **Cancel**. The Manager returns to the **Configuration | User Management | Groups** screen, and the **Current Groups** list is unchanged.

Configuration | User Management | Users

This section of the Manager lets you configure access, usage, and authentication parameters for users. Users inherit parameters from the specific group to which they belong.

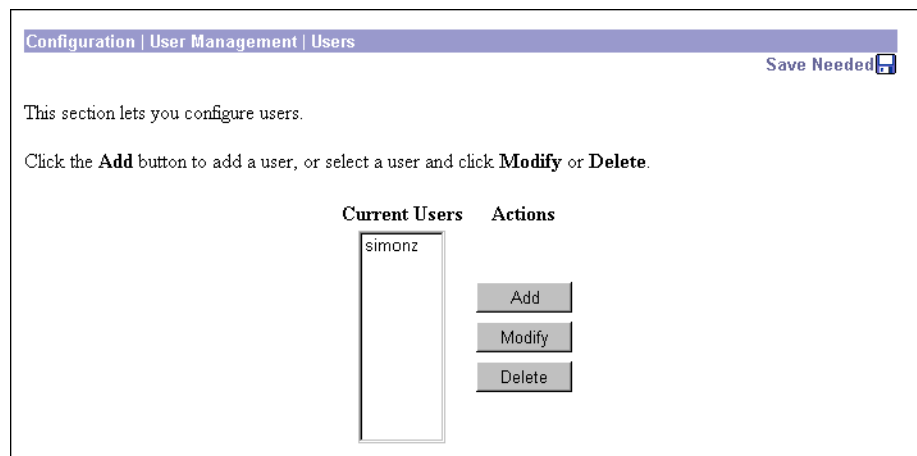
Configuring users in this section means configuring them in the VPN Concentrator internal authentication server. If you have not configured the internal authentication server, this screen displays a notice that includes a link to the **Configuration | System | Servers | Authentication** screen. The system also automatically configures the internal server when you add the first user.

See the discussion of groups and users under *User Management* at the beginning of this chapter.

Remember:

- You can configure a maximum of 100 groups and users (combined) in the VPN Concentrator internal server.
- A user can be a member of only one group.
- Users who are not members of a specific group are, by default, members of the base group. Therefore, to ensure maximum security and control, you should assign all users to appropriate specific groups, and you should configure base-group parameters carefully.

Figure 12-11: Configuration | User Management | Users screen



Current Users

The **Current Users** list shows configured users in alphabetical order. If no users have been configured, the list shows **--Empty--**.

Add / Modify / Delete

To configure a new user, click **Add**. The Manager opens the **Configuration | User Management | Users | Add** screen.

To modify a user that has been configured, select the user from the list and click **Modify**. The Manager opens the **Configuration | User Management | Users | Modify** screen.

To remove a user that has been configured, select the user from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining users in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | User Management | Users | Add or Modify

These Manager screens let you:

Add: Configure a new user and that user's parameters on the internal authentication server.

Modify: Change parameters for a user that you have previously configured on the internal authentication server. The screen title identifies the user you are modifying.

For many of these parameters, you can simply specify that the user "inherit" parameters from a group; and a user can be assigned either to a configured group or to the base group. Users who are not members of a configured group are, by default, members of the base group.

On this screen, you configure four kinds of parameters:

- **Identity Parameters:** name, password, group, and IP address.
- **General Parameters:** access, performance, and allowed tunneling protocols.
- **IPSec Parameters:** IP Security tunneling protocol.
- **PPTP/L2TP Parameters:** PPTP and L2TP tunneling protocols.

Tip:

To streamline the configuration process, just fill in the **Identity Parameters** tab (assigning the user to a configured group), and click **Add**. Then select the user and click **Modify**. The user inherits the group parameters, and the **Modify** screen shows group parameters instead of base-group parameters.

Before configuring these parameters, you should configure the base-group parameters on the **Configuration | User Management | Base Group** screen, and configure group parameters on the **Configuration | User Management | Groups** screen.

Using the tabs

This screen includes four tabbed sections. Click each tab to display its parameters. As you move from tab to tab, the Manager retains your settings. When you have finished setting parameters on all tabbed sections, click **Add / Apply** or **Cancel**.

Figure 12-12: Configuration | User Management | Users | Add or Modify screen, Identity tab

Configuration | User Management | Users | Modify simonz

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPSec PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
User Name	<input type="text"/>	Enter a unique user name.
Password	<input type="password"/>	Enter the user's password. The password must satisfy the group password requirements.
Verify	<input type="password"/>	Verify the user's password.
Group	--Base Group--	Enter the group to which this user belongs.
IP Address	<input type="text"/>	Enter the IP address assigned to this user.
Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.

Add Cancel

Identity Parameters tab

This tab lets you configure the name, password, group, and IP address for this user.

User Name

Enter a unique name for this user. Maximum is 32 characters, case-sensitive.

If you change this name, this user profile *replaces* the existing profile.

Password

Enter a unique password for this user. The minimum length must satisfy the minimum for the group to which you assign this user (base group or specific group). Maximum is 32 characters, case-sensitive. The field displays only asterisks.

Verify

Re-enter the user password to verify it. The field displays only asterisks.

Group

Click the drop-down menu button and select the group to which you assign this user. The list shows specific groups you have configured, plus:

--Base Group-- = The default group with its base-group parameters.

IP Address

Enter the IP address, in dotted decimal notation, assigned to this user. Enter this address only if you assign this user to the base group or an internally configured group, and if you configure **Use Address from Authentication Server** on the **Configuration | System | Address Management | Assignment** screen. Otherwise, leave this field blank.

Subnet Mask

Enter the subnet mask, in dotted decimal notation, assigned to this user. Enter this mask only if you configure an IP address above; otherwise leave this field blank.

Figure 12-13: Configuration | User Management | Users | Add or Modify screen, General tab

Configuration | User Management | Users | Modify simonz

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity
General
IPSec
PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this user can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

Add
Cancel

General Parameters tab

This tab lets you configure general access, performance, and allowed tunneling protocols that apply to this user.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to group parameters: Does this specific user inherit the given setting from the group?
 - **Add** screen = inherit base-group parameter setting.
 - **Modify** screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the box (default). To override the group setting, clear the box. If you clear the check box, you must enter or change any corresponding **Value** field; do not leave the field blank.

- The **Value** column thus shows either group parameter settings that also apply to this user (**Inherit?** checked), or unique parameter settings configured for this user (**Inherit?** cleared). You cannot configure a grayed-out parameter.

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Access Hours

Click the drop-down menu button and select the named hours when this user can access the VPN Concentrator. Configure access hours on the **Configuration | Policy Management | Access Hours** screen. Default entries are:

-No Restrictions- = No named access hours applied, which means that there are no restrictions on access hours.

Never = No access at any time.

Business Hours = Access 9 a.m. to 5 p.m., Monday through Friday.

Additional named access hours that you have configured also appear on the list.

Simultaneous Logins

Enter the number of simultaneous logins permitted for this user. The minimum is 0, which disables login and prevents user access. While there is no maximum limit, allowing several could compromise security and affect performance.

Idle Timeout

Enter this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To disable timeout and allow an unlimited idle period, enter 0.

Maximum Connect Time

Enter this user's maximum connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, enter 0.

Filter

Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the VPN Concentrator, based on criteria such as source address, destination address, and protocol. Cisco supplies three default filters, which you can modify. To configure filters and rules, see the **Configuration | Policy Management | Traffic Management** screens.

Click the drop-down menu button and select the filter to apply to this user:

--None-- = No filter applied, which means there are no restrictions on tunneled data traffic.

Private (Default) = Allow all packets except source-routed IP packets. (This is the default filter for the private Ethernet interface.)

Public (Default) = Allow inbound and outbound tunneling protocols plus ICMP and VRRP. Allow fragmented IP packets. Drop everything else, including source-routed packets. (This is the default filter for the public Ethernet interface.)

External (Default) = No rules applied to this filter. Drop all packets. (This is the default filter for the external Ethernet interface.)

Additional filters that you have configured also appear on the list.

SEP Card Assignment

The VPN Concentrator can contain up to four SEP (Scalable Encryption Processing) modules that handle encryption functions, which are compute-intensive. Two SEP modules handle up to 5000 sessions (users)—the system maximum. Two additional modules can provide automatic failover for the first two. This parameter lets you configure the load on each SEP module.

Check the box to assign this user to a given SEP module. If your system does not have a given SEP module, the parameter is ignored.

Tunneling Protocols

Check the desired boxes to select the VPN tunneling protocols that this user can use. Configure parameters on the **IPSec** or **PPTP/L2TP** tabs as appropriate. Users can use only the selected protocols.

You cannot check both **IPSec** and **L2TP over IPSec**. The IPSec parameters differ for these two protocols, and you cannot configure a single user for both.

PPTP = Point-to-Point Tunneling Protocol. PPTP is a client-server protocol, and it is popular with Microsoft clients. Microsoft Dial-Up Networking (DUN) 1.2 and 1.3 under Windows 95/98 support it, as do versions of Windows NT 4.0 and Windows 2000.

L2TP = Layer 2 Tunneling Protocol. L2TP is a client-server protocol. It combines many features from PPTP and L2F (Layer 2 Forwarding).

IPSec = IP Security Protocol. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec. The Cisco VPN 3000 Client is an IPSec client

specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients.

L2TP over IPSec = L2TP using IPSec for security. L2TP packets are encapsulated within IPSec, thus providing an additional authentication and encryption layer for security. L2TP over IPSec is a client-server protocol, and it provides interoperability with the Windows 2000 VPN client and other compliant remote-access clients.

Note: If no protocol is selected, this user cannot access or use the VPN.

Figure 12-14: Configuration | User Management | Users | Add or Modify screen, IPSec tab

Configuration | User Management | Users | Modify simonz

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General **IPSec** PPTP/L2TP

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the IPSec Security Association assigned to this user.
Store Password on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.

Add Cancel

IPSec Parameters tab

This tab lets you configure IP Security Protocol parameters that apply to this user. If you checked **IPSec** or **L2TP over IPSec** under **Tunneling Protocols** on the **General Parameters** tab, configure this section.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to group parameters: Does this specific user inherit the given setting from the group?
 - **Add** screen = inherit base-group parameter setting.
 - **Modify** screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the box (default). To override the group setting, clear the box. If you clear the check box, you must enter or change any corresponding **Value** field; do not leave the field blank.

- The **Value** column thus shows either group parameter settings that also apply to this user (**Inherit?** checked), or unique parameter settings configured for this user (**Inherit?** cleared). You cannot configure a grayed-out parameter.

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

IPSec SA

Click the drop-down menu button and select the IPSec Security Association (SA) assigned to this IPSec user. During tunnel establishment, the user client and server negotiate a Security Association that governs authentication, encryption, encapsulation, key management, etc. You configure IPSec Security Associations on the **Configuration | Policy Management | Traffic Management | Security Associations** screens.

To use IPSec with remote-access clients, you must assign an SA. With IPSec LAN-to-LAN connections, the system ignores this selection and uses parameters from the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN** screens.

The VPN Concentrator supplies these default selections:

--None-- = No SA assigned.

ESP-DES-MD5 = This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.

ESP/IKE-3DES-MD5 = This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-3DES-NONE = This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.

ESP-L2TP-TRANSPORT = This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the **L2TP over IPSec** tunneling protocol.

Additional SAs that you have configured also appear on the list.

Store Password on Client

Check the box to allow this IPSec user (client) to store the login password on the client system. If you do not allow password storage, IPSec users must enter their password each time they seek access to the VPN. For maximum security, we recommend that you *not allow* password storage.

Figure 12-15: Configuration | User Management | Users | Add or Modify screen, PPTP/L2TP tab

Configuration | User Management | Users | Modify simonz

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec **PPTP/L2TP**

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] <input type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking all options means that no authentication is required.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] <input type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	<input checked="" type="checkbox"/>	Enter the authentication protocols this user is allowed to use. This is used to <i>remove</i> protocols from the list of acceptable authentication protocols. Unchecking all options means that no authentication is required.

Add Cancel

PPTP/L2TP Parameters tab

This tab lets you configure PPTP and L2TP parameters that apply to this user. During tunnel establishment, the user client and server negotiate access and usage based on these parameters. Only clients that meet these criteria are allowed access. If you checked **PPTP**, **L2TP**, or **L2TP over IPsec** under **Tunneling Protocols** on the **General Parameters** tab, configure these parameters.

Value / Inherit?

On this tabbed section:

- The **Inherit?** check box refers to group parameters: Does this specific user inherit the given setting from the group?
 - **Add** screen = inherit base-group parameter setting.
 - **Modify** screen = inherit assigned-group parameter setting, which can be the base group or a configured group.

To inherit the group setting, check the box (default). To override the group setting, clear the box. If you clear the check box, you must enter or change any corresponding **Value** field; do not leave the field blank.

- The **Value** column thus shows either group parameter settings that also apply to this user (**Inherit?** checked), or unique parameter settings configured for this user (**Inherit?** cleared). You cannot configure a grayed-out parameter.

Note: The setting of the **Inherit?** check box takes priority over an entry in a **Value** field. Examine this box before continuing and be sure its setting reflects your intent.

Use Client Address

Check the box to accept and use an IP address that this user (client) supplies. A client must have an IP address to function as a tunnel endpoint; but for maximum security, we recommend that you control IP address assignment and *not allow* client-specified IP addresses.

Make sure the setting here is consistent with the setting for **Use Client Address** on the **Configuration | System | Address Management | Assignment** screen.

PPTP Authentication Protocols

Check the boxes for the authentication protocols that this PPTP user (client) can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, PPTP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure. You can allow a user to use *fewer* protocols than the assigned group, but not more. You cannot allow a grayed-out protocol.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol.

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP.

EAP = Extensible Authentication Protocol. This protocol supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption).

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths.

L2TP Authentication Protocols

Check the boxes for the authentication protocols that this L2TP user (client) can use. To establish and use a VPN tunnel, users should be authenticated according to some protocol.

Caution: Unchecking *all* authentication options means that *no* authentication is required. That is, L2TP users can connect with *no* authentication. This configuration is allowed so you can test connections, but it is not secure.

These choices specify the allowable authentication protocols in order from least secure to most secure. You can allow a user to use *fewer* protocols than the assigned group, but not more. You cannot allow a grayed-out protocol.

PAP = Password Authentication Protocol. This protocol passes cleartext username and password during authentication and is not secure. We strongly recommend that you *not allow* this protocol.

CHAP = Challenge-Handshake Authentication Protocol. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. It is more secure than PAP.

EAP = Extensible Authentication Protocol. This protocol supports **-MD5** (MD5-Challenge) authentication, which is analogous to the CHAP protocol, with the same level of security.

MSCHAPv1 = Microsoft Challenge-Handshake Authentication Protocol version 1. This protocol is similar to, but more secure than, CHAP. In response to the server challenge, the client returns the encrypted [challenge plus encrypted password], with a cleartext username. Thus the server stores—and compares—only encrypted passwords, rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE (Microsoft Point-to-Point Encryption).

MSCHAPv2 = Microsoft Challenge-Handshake Authentication Protocol version 2. This protocol is even more secure than MSCHAPv1. It requires mutual client-server authentication, uses session-unique keys for data encryption by MPPE, and derives different encryption keys for the send and receive paths.

Add or Apply / Cancel

When you finish setting or changing parameters on all tabs, click **Add** or **Apply** at the bottom of the screen to **Add** this user to the list of configured internal users, or to **Apply** your changes. Both actions include your settings in the active configuration. The Manager returns to the **Configuration | User Management | Users** screen. Any new users appear in alphabetical order in the **Current Users** list.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | User Management | Users** screen, and the **Current Users** list is unchanged.

End of Chapter



Policy Management

Managing a VPN, and protecting the integrity and security of network resources, includes carefully designing and implementing policies that govern who can use the VPN, when, and what data traffic can flow through it. User management deals with “who can use it”; see the *User Management* section for that discussion. Policy management deals with “when” and “what data traffic can flow through it”; this section covers those topics.

You configure “when” under **Access Hours**, and it’s simple: when can remote users access the VPN.

You configure “what data traffic can flow through it” under **Traffic Management**, and it’s a bit more complex. The Cisco VPN 3000 Concentrator hierarchy is straightforward, however: you use *filters* that consist of *rules*; and for IPSec rules, you apply *Security Associations* (SAs). Therefore, you first construct (configure) rules and SAs, then use them to construct filters.

Basically, a *filter* determines whether to forward or drop a data packet coming through the system. It examines the data packet according to one or more *rules*—direction, source address, destination address, ports, and protocol—which determine whether to forward, apply IPSec and forward, or drop. And it examines the rules in the order they are arranged on the filter.

You apply filters to Ethernet interfaces, and thus govern *all* traffic through an interface. You also apply filters to groups and users, and thus govern *tunneled* traffic through an interface.

With IPSec, the VPN Concentrator negotiates *Security Associations* during tunnel establishment that govern authentication, key management, encryption, encapsulation, etc. Thus IPSec also determines how to transform a data packet before forwarding it. You apply Security Associations to IPSec rules when you include those rules in a filter, and you apply SAs to groups and users.

The VPN Concentrator also lets you create network lists, which are lists of network addresses that are treated as a single object. These lists simplify the configuration of rules for complex networks. You can also use them to configure split tunneling for groups and users, and to configure IPSec LAN-to-LAN connections.

To fully configure the VPN Concentrator, you should first develop policies (network lists, rules, SAs, and filters), since they affect Ethernet interfaces, groups, and users. And once you have developed policies, we recommend that you configure and apply filters to interfaces before you configure groups and users.

Traffic management on the VPN Concentrator also includes NAT (Network Address Translation) functions that translate private network addresses into legitimate public network addresses. Again, you develop rules to configure and use NAT.

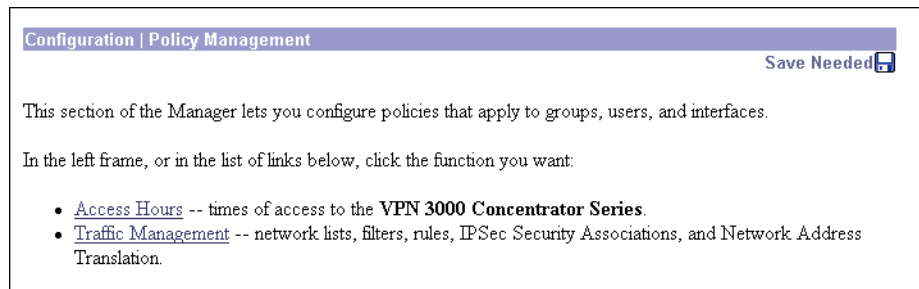
Configuration | Policy Management

This section of the Manager lets you configure policies that apply to groups, users, and VPN Concentrator Ethernet interfaces.

Policies govern:

- **Access Hours:** when remote users can access the VPN Concentrator.
- **Traffic Management:** what data traffic can flow through the VPN Concentrator, as governed by:
 - **Network Lists:** lists of networks grouped as single objects.
 - **Rules:** detailed parameters that govern the handling of data packets.
 - **SAs:** IPSec Security Associations.
 - **Filters:** structures for applying aggregated rules.
 - **NAT:** Network Address Translation.

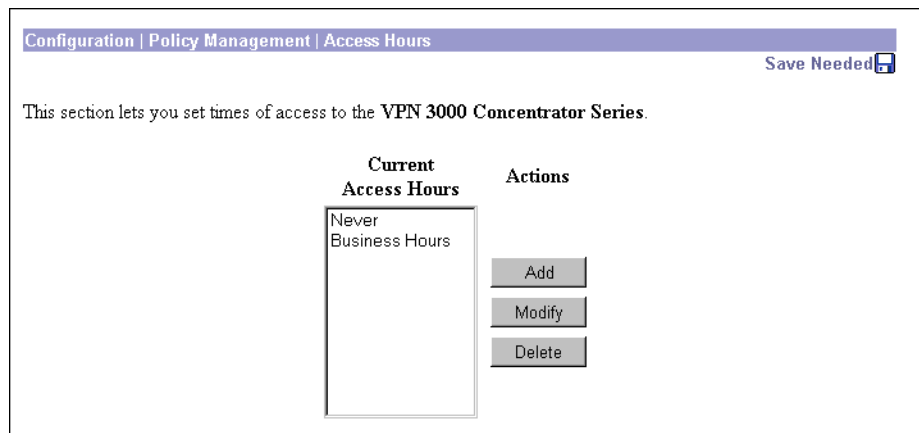
Figure 13-1: Configuration | Policy Management screen



Configuration | Policy Management | Access Hours

This section of the Manager lets you configure access times, to control when remote-access groups and users can access the VPN Concentrator. You assign access hours to groups and users under **Configuration | User Management**. Access hours don't apply to LAN-to-LAN connections.

Figure 13-2: Configuration | Policy Management | Access Hours screen



Current Access Hours

The **Current Access Hours** list shows the names of configured access times. The Cisco-supplied default access times are:

Never = Never. No access at any time.

Business Hours = Monday through Friday, 9 a.m. to 5 p.m.

Additional access times that you configure appear in the list.

Add / Modify / Delete

To configure and add a new access time to the list, click **Add**. The Manager opens the **Configuration | Policy management | Access Hours | Add** screen.

To modify a configured access time, select the entry from the list and click **Modify**. The Manager opens the **Configuration | Policy management | Access Hours | Modify** screen.

To remove a configured access time, select the entry from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the **Current Access Hours** list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Access Hours | Add or Modify

These Manager screens let you:

Add: Configure and add a new access time to the list of configured access times.

Modify: Modify a configured access time. Changing an access time has no effect on connected users, since the parameter is checked only when the tunnel is established. The change affects subsequent connections, however.

Figure 13-3: Configuration | Policy Management | Access Hours | Add or Modify screens

The figure shows two overlapping screenshots of the configuration interface. The top screenshot, titled 'Configuration | Policy Management | Access Hours | Modify', displays the text 'Modify a configured set of access hours.' The bottom screenshot, titled 'Configuration | Policy Management | Access Hours | Add', displays the text 'Configure and add a new set of access hours.' Below this text is a form with the following fields:

- Name:** A text input field with the instruction 'Specify a unique name for this set of access hours.'
- Sunday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Monday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Tuesday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Wednesday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Thursday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Friday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.
- Saturday:** A dropdown menu set to 'during', followed by two time input fields: '00:00:00' and '23:59:59'.

At the bottom of the 'Add' screen are two buttons: 'Add' and 'Cancel'.

Name

Enter a unique name for this set of access hours. Maximum is 48 characters.

Sunday - Saturday

For each day of the week, click the drop-down menu button and select:

during = Allow access *during* the hours in the range (default).

except = Allow access at times *except* the hours in the range.

Enter or edit hours in the range fields. Times are inclusive: starting time through ending time. Enter times as HH:MM:SS. Use 24-hour notation; e.g., enter 5:30 p.m. as 17:30. By default, all ranges are 00:00:00 to 23:59:59.

Add or Apply / Cancel

To add this access time to the list, click **Add**. Or to apply your changes for this access time, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | Policy Management | Access Hours** screen. Any new entry appears in the **Current Access Times** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Access Hours** screen, and the **Current Access Times** list is unchanged.

Configuration | Policy Management | Traffic Management

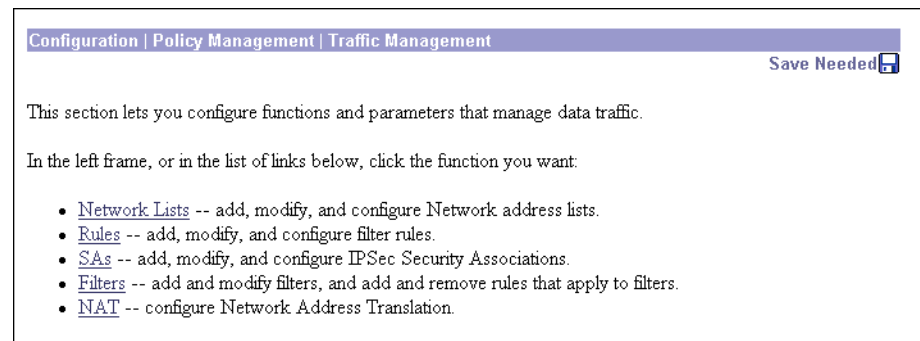
This section of the Manager lets you configure network lists, rules, filters, Security Associations, and network address translation, which let you control the data traffic through the VPN Concentrator.

Network lists let you treat lists of network addresses as a single object, thus simplifying the configuration of rules for complex networks. Filters consist of rules; and IPSec rules (rules in which you configure an **Apply IPSec** action) also have Security Associations. Therefore you first configure any network lists, then rules and SAs, and finally filters.

A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the action specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the default action specified in the filter.

You apply filters to interfaces under **Configuration | Interfaces**, and these are the most important filters for security since they apply to *all* traffic. You also apply filters to groups and users under **Configuration | User Management**; these filters apply to *tunneled* traffic only.

Figure 13-4: Configuration | Policy Management | Traffic Management screen



Configuration | Policy Management | Traffic Management | Network Lists

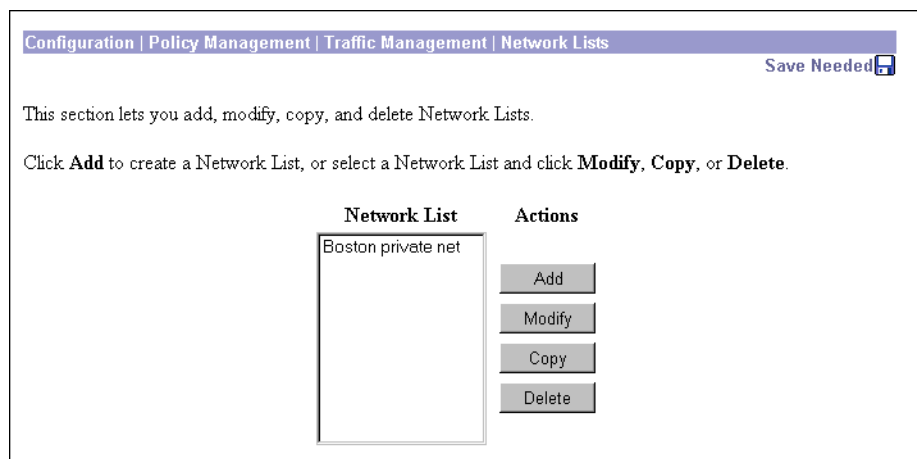
This section of the Manager lets you configure network lists, which are lists of networks that are grouped as single objects. Network lists make configuration easier: for example, you can use a network list to configure one filter rule for a set of networks rather than configuring separate rules for each network.

You can use network lists in configuring filter rules (see **Configuration | Policy Management | Traffic Management | Rules**). You can also use them to configure split tunneling for groups and users (see **Configuration | User Management**), and to configure IPSec LAN-to-LAN connections (see **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN**).

The Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and **Inbound RIP** must be enabled on that interface.

A single network list can contain a maximum of 200 network entries. The Manager does not limit the number of network lists you can configure.

Figure 13-5: Configuration | Policy Management | Traffic Management | Network Lists screen



Network List

The **Network List** field shows the names of the network lists you have configured. If no lists have been configured, the field shows **--Empty--**.

Add / Modify / Copy / Delete

To configure and add a new network list, click **Add**. The Manager opens the **Configuration | Policy Management | Traffic Management | Network Lists | Add** screen.

To modify a configured network list, select the list and click **Modify**. The Manager opens the **Configuration | Policy Management | Traffic Management | Network Lists | Modify** screen.

To copy a configured network list, modify it, and save it with a new name, select the list and click **Copy**. See the **Configuration | Policy Management | Traffic Management | Network Lists | Copy** screen.

To delete a configured network list, select the list and click **Delete**. If the network list is configured on a filter rule or an IPSec LAN-to-LAN connection, the Manager displays an error message indicating the

action to take before you can delete the list. *Otherwise, there is no confirmation or undo.* The Manager deletes the list, refreshes the screen, and shows the remaining network lists.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Network Lists | Add, Modify, or Copy

These screens let you:

Add: Configure and add a new network list.

Modify: Modify a previously configured network list.

Copy: Copy a configured network list, modify its parameters, save it with a new name, and add it to the configured network lists.

On the **Add** and **Modify** screens, the Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and **Inbound RIP** must be enabled on that interface.

Figure 13-6: Configuration | Policy Management | Traffic Management | Network Lists | Add, Modify, or Copy screens

The figure shows three overlapping screenshots of the configuration interface for Network Lists:

- Top Screenshot (Copy):** The breadcrumb trail is "Configuration | Policy Management | Traffic Management | Network List | Copy". The main text says "Copy a configured Network List."
- Middle Screenshot (Modify):** The breadcrumb trail is "Configuration | Policy Management | Traffic Management | Network Lists | Modify". The main text says "Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface."
- Bottom Screenshot (Add):** The breadcrumb trail is "Configuration | Policy Management | Traffic Management | Network Lists | Add". The main text says "Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface." Below this text is a form with:
 - A text input field labeled "List Name".
 - A large text area labeled "Network List".
 - Three buttons at the bottom: "Add", "Cancel", and "Generate Local List".

To the right of the "Add" screenshot, there is explanatory text and a list of instructions:

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.mnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

List Name

Enter a unique name for this network list. Maximum 48 characters, case-sensitive. Spaces are allowed.

If you use the **Generate Local List** feature on the **Add** screen, enter this name *after* the system generates the network list.

Network List

Enter the networks in this network list. Enter each network on a single line using the format `n.n.n.n/w.w.w.w`, where `n.n.n.n` is a network IP address and `w.w.w.w` is a wildcard mask.

Note: Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, `10.10.1.0/0.0.0.255` = all `10.10.1.nnn` addresses.

If you omit the wildcard mask, the Manager supplies the default wildcard mask for the class of the network address. For example, `192.168.12.0` is a Class C address, and default wildcard mask is `0.0.0.255`.

You can include a maximum of 200 network/wildcard entries in a single network list.

Generate Local List

On the **Add** or **Modify** screen, click this button to have the Manager automatically generate a network list containing the first 200 private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table (see **Monitoring | Routing Table**), and **Inbound RIP** must be enabled on that interface (see **Configuration | Interfaces**). The Manager refreshes the screen after it generates the list, and you can then edit the **Network List** and enter a **List Name**.

Note: The generated list replaces any existing entries in the **Network List**.

Add or Apply / Cancel

To add this network list to the configured network lists, click **Add**. Or to apply your changes to this network list, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | Policy Management | Traffic Management | Network Lists** screen. Any new entry appears at the bottom of the **Network List** field.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

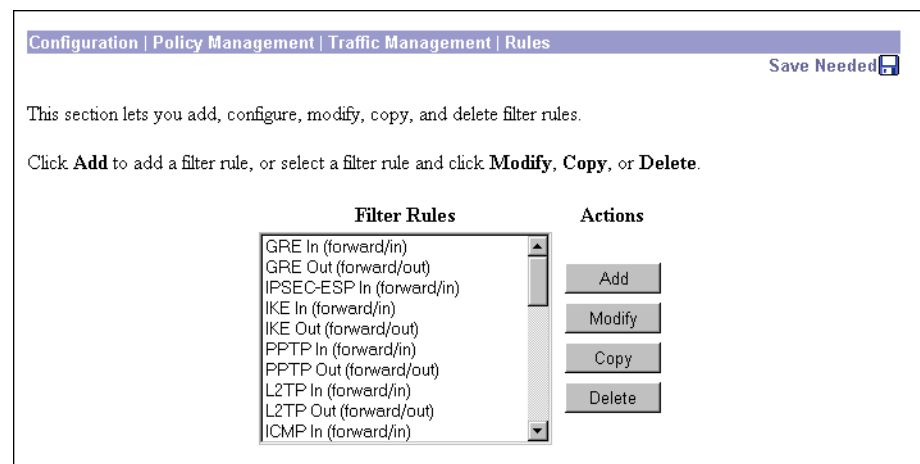
To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Network Lists** screen, and the **Network Lists** field is unchanged.

Configuration | Policy Management | Traffic Management | Rules

This section of the Manager lets you add, configure, modify, copy, and delete filter rules. You use rules to construct filters.

Caution: The Cisco-supplied default rules are intended as templates that you should examine and modify to fit your network and security needs. Unmodified, or incorrectly applied, they could present security risks. You should also be especially careful about adding rules to the **Public (Default)** filter. For example, the default **Incoming HTTP** rules are intended to allow an administrator outside the private network to manage the VPN Concentrator with a browser. Unmodified, they could allow browser connections to any system on the private network. If you apply these rules to a filter, you should at least change the **Source** and **Destination Address** to limit the connections.

Figure 13-7: Configuration | Policy Management | Traffic Management | Rules screen



Filter Rules

The **Filter Rules** list shows the configured rules that are available to apply to filters. The list shows the rule name and the action/direction in parentheses. The rules are listed in the order they are configured.

Cisco supplies several default rules that you can modify and use. See Table 13-1 for their parameters, and see **Configuration | Policy Management | Traffic Management | Rules | Add** for explanations of the parameters.

For all the default rules except **VRRP In** and **Out**, these parameters are identical:

Action = Forward

Source Address = Use IP Address/Wildcard-Mask = 0.0.0.0/255.255.255.255 = any address

Destination Address = Use IP Address/Wildcard-Mask = 0.0.0.0/255.255.255.255 = any address

*For maximum security and control, we recommend that you change the **Source Address and Destination Address** to fit your network addressing and security scheme.*

Table 13-1: Cisco-supplied default filter rules

Filter Rule Name	Direction	Protocol	TCP Connection	TCP/UDP Source Port	TCP/UDP Destination Port	ICMP Packet Type
Any In	Inbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
Any Out	Outbound	Any	Don't Care	Range 0-65535	Range 0-65535	0-255
CRL over LDAP In	Inbound	TCP	Don't Care	LDAP (389)	Range 0-65535	
CRL over LDAP Out	Outbound	TCP	Don't Care	Range 0-65535	LDAP (389)	
GRE In	Inbound	GRE				
GRE Out	Outbound	GRE				
ICMP In	Inbound	ICMP				0-18
ICMP Out	Outbound	ICMP				0-18
IKE In	Inbound	UDP		Range 0-65535	IKE (500)	
IKE Out	Outbound	UDP		IKE (500)	Range 0-65535	
Incoming HTTP In	Inbound	TCP	Don't Care	Range 0-65535	HTTP (80)	
Incoming HTTP Out	Outbound	TCP	Don't Care	HTTP (80)	Range 0-65535	
Incoming HTTPS In	Inbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	
Incoming HTTPS Out	Outbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	
IPSec-ESP In	Inbound	ESP				
L2TP In	Inbound	UDP		Range 0-65535	L2TP (1701)	
L2TP Out	Outbound	UDP		L2TP (1701)	Range 0-65535	
LDAP In	Inbound	TCP	Don't Care	Range 0-65535	LDAP (389)	
LDAP Out	Outbound	TCP	Don't Care	LDAP (389)	Range 0-65535	
OSPF In	Inbound	OSPF				
OSPF Out	Outbound	OSPF				
Outgoing HTTP In	Inbound	TCP	Don't Care	HTTP (80)	Range 0-65535	
Outgoing HTTP Out	Outbound	TCP	Don't Care	Range 0-65535	HTTP (80)	

Table 13-1: Cisco-supplied default filter rules (continued)

Filter Rule Name	Direction	Protocol	TCP Connection	TCP/UDP Source Port	TCP/UDP Destination Port	ICMP Packet Type
Outgoing HTTPS In	Inbound	TCP	Don't Care	HTTPS (443)	Range 0-65535	
Outgoing HTTPS Out	Outbound	TCP	Don't Care	Range 0-65535	HTTPS (443)	
PPTP In	Inbound	TCP	Don't Care	Range 0-65535	PPTP (1723)	
PPTP Out	Outbound	TCP	Don't Care	PPTP (1723)	Range 0-65535	
RIP In	Inbound	UDP		RIP (520)	RIP (520)	
RIP Out	Outbound	UDP		RIP (520)	RIP (520)	
Telnet/SSL In	Inbound	TCP	Don't Care	Range 0-65535	Telnet/SSL (992)	
Telnet/SSL Out	Outbound	TCP	Don't Care	Telnet/SSL (992)	Range 0-65535	
VRRP In *	Inbound	Other 112				
VRRP Out *	Outbound	Other 112				

*For **VRRP In** and **VRRP Out**, the **Destination Address** is 224.0.0.18/0.0.0.0, which is the IANA-assigned IP multicast address for VRRP.

Add / Modify / Copy / Delete

To configure a new rule, click **Add**. The Manager opens the **Configuration | Policy Management | Traffic Management | Rules | Add** screen.

To modify a rule that has been configured, select the rule from the list and click **Modify**. The Manager opens the **Configuration | Policy Management | Traffic Management | Rules | Modify** screen.

To copy a configured rule, modify it, and save it with a new name, select the rule from the list and click **Copy**. See the **Configuration | Policy Management | Traffic Management | Rules | Copy** screen.

To delete a configured rule, select the rule from the list and click **Delete**.

- If the rule *is not* being used in a filter, the Manager deletes the rule, refreshes the screen, and shows the remaining rules in the list. *There is no confirmation or undo.*
- If the rule *is* being used in a filter, the Manager asks you to confirm the deletion. See the **Configuration | Policy Management | Traffic Management | Rules | Delete** screen.
- You cannot delete a rule that is configured as part of a LAN-to-LAN connection. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Note: *Deleting* a rule deletes it from every filter that uses it and deletes it from the VPN Concentrator active configuration. To *remove* a rule from a filter but retain it in the active configuration, see the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Rules | Add, Modify, or Copy

These Manager screens let you:

Add: Configure and add a new filter rule to the list of filter rules.

Modify: Modify a previously configured filter rule.

Copy: Copy a configured rule, modify its parameters, save it with a new name, and add it to the list of filter rules.

The VPN Concentrator applies rule parameters to data traffic (packets) in the order presented on this screen (from **Protocol** down) to see if they match. If all parameters match, the system takes the specified **Action**. If at least one parameter does not match, the system ignores the rest of this rule and examines the packet according to the next rule, and so forth.

Note: On the **Modify** screen, any changes take effect as soon as you click **Apply**. Changes affect *all* filters that use this rule. If this rule is being used by an active filter, changes may affect tunnel traffic.

Figure 13-8: Configuration | Policy Management | Traffic Management | Rules | Add, Modify, or Copy screen

Configuration | Policy Management | Traffic Management | Rules | Copy

Copy a rule.

Configuration | Policy Management | Traffic Management | Rules | Modify

Modify a filter rule.

Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name	<input type="text"/>	Name of this filter rule. The name must be unique.
Direction	<input type="text" value="Inbound"/>	Select the data direction to which this rule applies.
Action	<input type="text" value="Drop"/>	Specify the action to take when this filter rule applies.

Protocol	<input type="text" value="Any"/>	Select the protocol to which this rule applies. For
or Other	<input type="text"/>	Other protocols, enter the protocol number.
TCP Connection	<input type="text" value="Don't Care"/>	Select whether this rule should apply to an established TCP connection.

Source Address

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the source network address list or the IP address and wildcard mask that this rule checks.
IP Address	<input type="text" value="0.0.0.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard-mask	<input type="text" value="255.255.255.255"/>	

Destination Address

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the destination network address list or the IP address and wildcard mask that this rule checks.
IP Address	<input type="text" value="0.0.0.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard-mask	<input type="text" value="255.255.255.255"/>	

TCP/UDP Source Port

Port	<input type="text" value="Range"/>	For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.
or Range	<input type="text" value="0"/> to <input type="text" value="65535"/>	

TCP/UDP Destination Port

Port	<input type="text" value="Range"/>	For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.
or Range	<input type="text" value="0"/> to <input type="text" value="65535"/>	

ICMP Packet Type

	<input type="text" value="0"/> to <input type="text" value="255"/>	For ICMP, specify the range of ICMP packet types that this rule checks.
--	--	---

Rule Name

Enter a unique name for this rule. Maximum is 48 characters.

Direction

Click the drop-down menu button and select the data direction to which this rule applies:

Inbound = Into the VPN Concentrator interface; or into the VPN tunnel from the remote client or host. (This is the default selection.)

Outbound = Out of the VPN Concentrator interface; or out of the VPN tunnel to the remote client or host.

Action

Click the drop-down menu button and select the action to take if the data traffic (packet) matches all parameters that follow. The choices are:

Drop = Discard the packet (the default selection).

Forward = Allow the packet to pass.

Drop and Log = Discard the packet and log a filter debugging event (FILTERDBG event class). See **Configuration | System | Events** and see note below.

Forward and Log = Allow the packet to pass and log a filter debugging event (FILTERDBG event class). See note below.

Apply IPSec = Apply IPSec to the packet; i.e. apply packet authentication, encryption, etc. according to parameters that are specified in a Security Association. You must configure a Security Association if you select this action. Also, you can assign an SA to this rule only if you select this (or the following) action; see **Configuration | Policy Management | Traffic Management | Security Associations**. See note below.

Apply IPSec and Log = Apply IPSec to the packet and log a filter debugging event (FILTERDBG event class). See notes below.

Notes: The **Log** actions are intended for use only while debugging filter activity. Since they generate and log an event for every matched packet, they consume significant system resources and may seriously degrade performance.

The **Apply IPSec** actions are for LAN-to-LAN traffic only, not for remote-access traffic. Remote-access IPSec traffic is authenticated and encrypted according to the SAs negotiated with the remote client (tunnel group) and user. In LAN-to-LAN connections, individual hosts on the LANs do not negotiate SAs. The VPN Concentrator automatically creates and applies appropriate rules when you create a LAN-to-LAN connection; see **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN**.

Protocol or Other

This parameter refers to the IANA (Internet Assigned Numbers Authority)-assigned protocol number in an IP packet. The descriptions below include the IANA number [in brackets] for reference.

Click the drop-down menu button and select the protocol to which this rule applies.

Any = Any protocol [255] (the default selection).

ICMP = Internet Control Message Protocol [1] (used by ping, for example). If you select this protocol, you should also configure **ICMP Packet Type**.

TCP = Transmission Control Protocol [6] (connection-oriented; e.g., FTP, HTTP, SMTP, and Telnet). If you select this protocol, you should configure **TCP Connection** and **TCP/UDP Source Port** or **Destination Port**.

EGP = Exterior Gateway Protocol [8] (used for routing to exterior networks).

IGP = Interior Gateway Protocol [9] (used for routing within a domain).

UDP = User Datagram Protocol [17] (connectionless; e.g., SNMP). If you select this protocol, you should also configure **TCP/UDP Source Port** or **Destination Port**.

ESP = Encapsulation Security Payload [50] (applies to IPSec).

AH = Authentication Header [51] (applies to IPSec).

GRE = Generic Routing Encapsulation [47] (used by PPTP).

RSVP = Resource Reservation Protocol [46] (reserves bandwidth on routers).

IGMP = Internet Group Management Protocol [2] (used in multicasting).

OSPF = Open Shortest Path First [89] (interior routing protocol).

Other = Other protocol not listed here. If you select **Other** here, you must enter the IANA-assigned protocol number in the **Other** field.

TCP Connection

Click the drop-down menu button and select whether this rule applies to packets from established TCP connections. For example, you might want a rule to forward only those TCP packets that originate from established connections on the public network interface, to provide maximum protection against “spoofing.” The choices are:

Established = Apply rule to packets from established TCP connections only.

Don't Care = Apply rule to any TCP packets, whether from established connections or new connections (the default selection).

Source Address

Specify the packet source address that this rule checks; i.e., the address of the sender.

Network List

Click the drop-down menu button and select the configured network list that specifies the source addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

Use IP Address/Wildcard-mask below, which lets you enter a network address.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard-mask** fields.

Note: An IP address is used with a *wildcard mask* to provide the desired granularity. A *wildcard mask* is the reverse of a *subnet mask*; i.e., the wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example:

0.0.0.0/255.255.255.255 = any address

10.10.1.35/0.0.0.0 = only 10.10.1.35

10.10.1.35/0.0.0.255 = all 10.10.1.nnn addresses

IP Address

Enter the source IP address in dotted decimal notation. Default is 0.0.0.0.

Wildcard-mask

Enter the source address wildcard mask in dotted decimal notation. Default is 255.255.255.255.

Destination Address

Specify the packet destination address that this rule checks; i.e., the address of the recipient.

Network List

Click the drop-down menu button and select the configured network list that specifies the destination addresses. A network list is a list of network addresses that are treated as a single object. See the **Configuration | Policy Management | Traffic Management | Network Lists** screens. Otherwise, you can select:

Use IP Address/Wildcard-mask below, which lets you enter a network address.

If you select a configured network list, the Manager ignores entries in the **IP Address** and **Wildcard-mask** fields.

See the *wildcard mask* note above.

IP Address

Enter the destination IP address in dotted decimal notation. Default is 0.0.0.0.

Wildcard-mask

Enter the destination address wildcard mask in dotted decimal notation. Default is 255.255.255.255.

TCP/UDP Source Port

If you select **TCP** or **UDP** under **Protocol** above, select the source port number that this rule checks.

Many different protocols or processes run in TCP or UDP environments, and each TCP or UDP process running on a network host is assigned a port number. Thus an IP address plus a port number uniquely identifies a process on a network host. Only TCP and UDP protocols use port numbers. The Internet

Assigned Numbers Authority (IANA) manages port numbers and classifies them as Well Known, Registered, and Dynamic (or Private). The Well Known ports are those from 0 through 1023; the Registered Ports are those from 1024 through 49151; and the Dynamic ports are those from 49152 through 65535.

Port or Range

Click the drop-down menu button and select the process (port number):

- ECHO (7)** = Used by ping for network testing.
- DISCARD (9)** = Used for network debugging and measurement.
- FTP-DATA (20)** = File Transfer Protocol, data port.
- FTP (21)** = File Transfer Protocol, control port.
- TELNET (23)** = Terminal emulation.
- SMTP (25)** = Simple Mail Transfer Protocol.
- DNS (53)** = Domain Name System.
- TFTP (69)** = Trivial File Transfer Protocol.
- FINGER (79)** = Network user inquiry.
- HTTP (80)** = Hypertext Transfer Protocol.
- POP3 (110)** = Post Office Protocol, version 3.
- NNTP (119)** = Network News Transfer Protocol.
- NTP (123)** = Network Time Protocol.
- NetBIOS Name Service (137)** = Network Basic Input Output System, host name assignment.
- NetBIOS (138)** = NetBIOS datagram service.
- NetBIOS Session (139)** = NetBIOS session management.
- IMAP (143)** = Internet Mail Access Protocol.
- SNMP (161)** = Simple Network Management Protocol.
- SNMP-TRAP (162)** = SNMP event or trap handling.
- BGP (179)** = Border Gateway Protocol.
- LDAP (389)** = Lightweight Directory Access Protocol.
- HTTPS (443)** = HTTP over a secure session (TLS/SSL).
- SMTPS (465)** = SMTP over a secure session (TLS/SSL).
- IKE (500)** = Internet Key Exchange Protocol (was ISAKMP/Oakley).
- SYSLOG (514)** = UNIX syslog server (UDP only).
- RIP (520)** = Routing Information Protocol (UDP only).
- NNTPS (563)** = NNTP over a secure session (TLS/SSL).
- LDAP/SSL (636)** = LDAP over a secure session (TLS/SSL).
- Telnet/SSL (992)** = Telnet over a secure session (TLS/SSL).
- LapLink (1547)** = Remote file management and mail.
- L2TP (1701)** = Layer 2 Tunneling Protocol.
- PPTP (1723)** = Point-to-Point Tunneling Protocol

Range = To specify a range of port numbers, or to specify a port not on the Cisco-supplied list, select **Range** here (the default selection) and enter—in the **Range [start] to [end]** fields—the inclusive range of port numbers that this rule applies to. To specify a single port number, enter the same number in both fields. Defaults are 0 to 65535 (all ports). The **Range** fields are ignored if you select a specific port from the drop-down list.

TCP/UDP Destination Port

If you select **TCP** or **UDP** under **Protocol** above, select the destination port number that this rule checks. See the explanation of port numbers under **TCP/UDP Source Port** above.

Port or Range

Click the drop-down menu button and select the process (port number). The choices are the same as listed under **TCP/UDP Source Port, Port or Range** above.

ICMP Packet Type

The ICMP protocol has many messages that are identified by a type number. For example:

```
0 = Echo Reply
8 = Echo
13 = Timestamp
14 = Timestamp Reply
17 = Address Mask Request
18 = Address Mask Reply
```

The Internet Assigned Numbers Authority (IANA) manages these ICMP type numbers.

If you selected **ICMP** under **Protocol** above, enter the range of ICMP packet type numbers that this rule applies to. To specify a single packet type, enter the same number in both fields. Defaults are 0 to 255 (all packet types). For example, to specify the **Timestamp** and **Timestamp Reply** types only, enter 13 to 14.

Add or Apply / Cancel

To add this rule to the list of configured filter rules, click **Add**. Or to apply your changes to this rule, click **Apply**. On the **Modify** screen, any changes take effect as soon as you click **Apply**. If the rule is being used by an active filter, changes may affect tunnel traffic. The Manager returns to the **Configuration | Policy Management | Traffic Management | Rules** screen. Any new rule appears in the **Filter Rules** list.

Reminder:

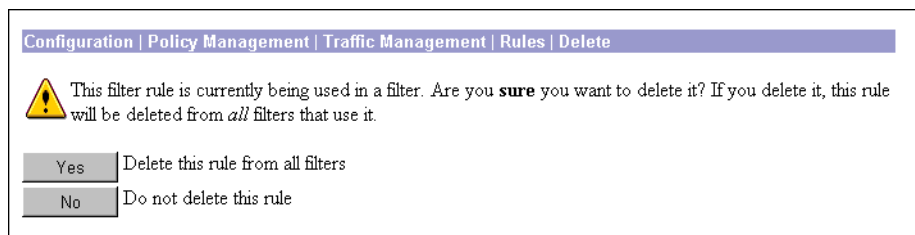
*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Rules** screen, and the **Filter Rules** list is unchanged.

Configuration | Policy Management | Traffic Management | Rules | Delete

This screen asks you to confirm deletion of a rule that is being used in a filter. Doing so deletes the rule from *all* filters that use it, and deletes it from the VPN Concentrator active configuration. To *remove* a rule from a filter but retain it in the active configuration, see the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen.

Figure 13-9: Configuration | Policy Management | Traffic Management | Rules | Delete screen



Note: The Manager deletes the rule from the filter as soon as you click **Yes**. If this rule is being used by an active filter, deletion may affect data traffic.

Yes / No

To delete this rule from all filters that use it, and delete it from the active configuration, click **Yes**. *There is no undo*. The Manager returns to the **Configuration | Policy Management | Traffic Management | Rules** screen and shows the remaining rules in the **Filter Rules** list.

Reminder: *To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To not delete this rule, click **No**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Rules** screen, and the **Filter Rules** list is unchanged.

Configuration | Policy Management | Traffic Management | Security Associations

This section of the Manager lets you add, configure, modify, and delete Security Associations (SAs). SAs apply only to IPSec tunnels. During tunnel establishment the two parties negotiate Security Associations that govern authentication, encryption, encapsulation, key management, etc. In other words, while rules and filters specify *what* traffic to manage, SAs tell *how* to do it.

IPSec configurations actually involve two SA negotiation phases: first, to establish the tunnel (the IKE SA); and second, to govern traffic within—the use of—the tunnel (the IPSec SA). You must configure IKE proposals before configuring Security Associations. See **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals**, or click the *IKE Proposals* link on this screen.

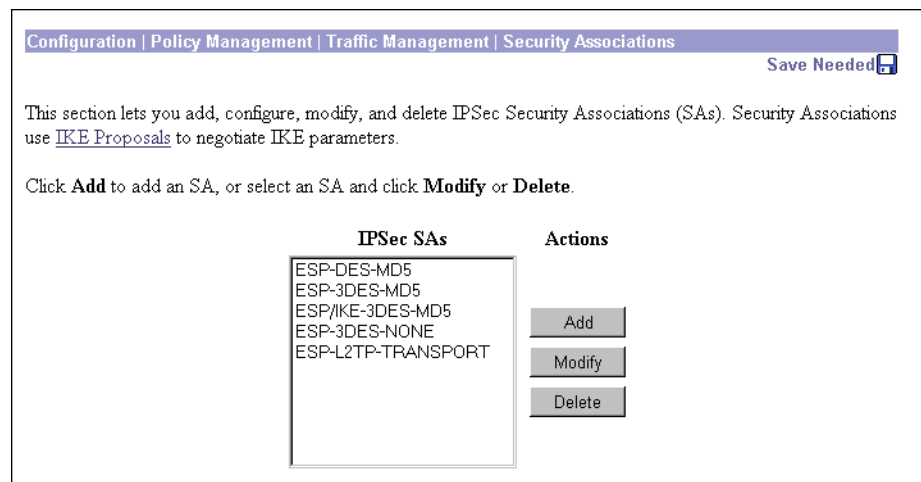
You apply SAs to filter rules that are configured with an **Apply IPSec** action, for LAN-to-LAN traffic. See **Configuration | Policy Management | Traffic Management | Rules**. The VPN Concentrator automatically creates and applies appropriate rules when you create a LAN-to-LAN connection; see **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN**. You also apply SAs to groups and users, for remote-access traffic, under the **IPSec Parameters** section on the appropriate **Configuration | User Management** screens.

You can use IPSec in both client-to-LAN (remote-access) configurations and LAN-to-LAN configurations. The Cisco VPN 3000 Client complies with the IPSec protocol and is specifically designed to work with the VPN Concentrator. However, the VPN Concentrator can establish IPSec connections with many protocol-compliant clients. Likewise, the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN devices (often called “secure gateways”). The instructions in this section, however, assume peer VPN Concentrators.

The Cisco VPN 3000 Client supports these IPSec attributes:

- Aggressive Negotiation Mode
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Group 1
- Encryption Algorithms:
 - DES-56
 - 3DES-168
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode

Figure 13-10: Configuration | Policy Management | Traffic Management | Security Associations screen



IPSec SAs

The **IPSec SAs** list shows the configured SAs that are available. The SAs are listed in the order they are configured.

Cisco supplies default SAs that you can use or modify; see Table 13-2. See **Configuration | Policy Management | Traffic Management | Security Associations | Add** for explanations of the parameters.

Table 13-2: Cisco-supplied default Security Associations

SA Name	ESP-DES-MD5	ESP-3DES-MD5	ESP/IKE-3DES-MD5	ESP-3DES-NONE	ESP-L2TP-TRANSPORT
Parameter					
Inheritance	From Rule	From Rule	From Rule	From Rule	From Rule
IPSec Parameters					
Authentication Algorithm	ESP/MD5/HMAC-128	ESP/MD5/HMAC-128	ESP/MD5/HMAC-128	None	ESP/MD5/HMAC-128
Encryption Algorithm	DES-56	3DES-168	3DES-168	3DES-168	DES-56
Encapsulation Mode	Tunnel	Tunnel	Tunnel	Tunnel	Transport
Perfect Forward Secrecy	Disabled	Disabled	Disabled	Disabled	Disabled
Lifetime Measurement	Time	Time	Time	Time	Time
Data Lifetime	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)	10000 KB (not relevant)
Time Lifetime	28800 sec	28800 sec	28800 sec	28800 sec	3600 sec
IKE Parameters					
IKE Peer	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Negotiation Mode	Main	Main	Main	Main	Main
Digital Certificate	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)	None (Use Preshared Keys)
IKE Proposal	IKE-DES-MD5	IKE-DES-MD5	IKE-3DES-MD5	IKE-3DES-MD5	IKE-3DES-MD5

Add / Modify / Delete

To configure a new SA, click **Add**. The Manager opens the **Configuration | Policy Management | Traffic Management | Security Associations | Add** screen.

To modify an SA that has been configured, select the SA from the list and click **Modify**. The Manager opens the **Configuration | Policy Management | Traffic Management | Security Associations | Modify** screen.

To delete a configured SA, select the SA from the list and click **Delete**.

- If the SA *has not* been assigned to a filter rule—even if it has been assigned to a group or user—the Manager deletes the SA, refreshes the screen, and shows the remaining SAs in the list. *There is no confirmation or undo.*
- If the SA *has* been assigned to a filter rule, the Manager asks you to confirm the deletion. See the **Configuration | Policy Management | Traffic Management | Security Associations | Delete** screen.
- You cannot delete an SA that is configured as part of a LAN-to-LAN connection. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Security Associations | Add or Modify

These screens let you:

Add: Configure and add a new Security Association to the list of configured SAs.

Modify: Modify a configured Security Association.

Note: On the **Modify** screen, any changes take effect as soon as you click **Apply**. If the SA is being used by an active filter rule or group, changes may affect tunnel traffic.

Figure 13-11: Configuration | Policy Management | Traffic Management | Security Associations | Add or Modify screen

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

Configuration | Policy Management | Traffic Management | Security Associations | Add

Configure and add a new Security Association.

SA Name Specify the name of this Security Association (SA).

Inheritance Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm Select the packet authentication algorithm to use.

Encryption Algorithm Select the ESP packet encryption algorithm to use.

Encapsulation Mode Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy Select the use of Perfect Forward Secrecy.

Lifetime Measurement Select the lifetime measurement of the IPSec keys.

Data Lifetime Specify the data lifetime in kilobytes (KB).

Time Lifetime Specify the time lifetime in seconds.

IKE Parameters

IKE Peer Specify the IKE Peer for a LAN-to-LAN connection.

Negotiation Mode Select the IKE Negotiation mode to use.

Digital Certificate Select the Digital Certificate to use.

IKE Proposal Select the IKE Proposal to use.

SA Name

Enter a unique name for this Security Association. Maximum is 48 characters.

Inheritance

This parameter specifies the granularity, or how many tunnels to build for this connection. Each tunnel uses a unique key.

Click the drop-down menu button and select:

From Rule = One tunnel for each *rule* in the connection. A rule can specify multiple networks, thus many hosts can use the same tunnel. This is the default—and recommended—selection.

From Data = One tunnel for every *address* pair within the address ranges specified in the rule. Each host uses a separate tunnel, and hence, separate keys. This selection is more secure but requires more processing overhead.

IPSec Parameters

These parameters apply to IPSec SAs, which are Phase 2 SAs negotiated under IPSec, where the two parties establish conditions for use of the tunnel.

Authentication Algorithm

This parameter specifies the data, or packet, authentication algorithm. Packet authentication proves that data comes from whom you think it comes from; it is often referred to as “data integrity” in VPN literature. The IPSec ESP (Encapsulating Security Payload) protocol provides both encryption and authentication.

Click the drop-down menu button and select the algorithm:

None = No data authentication.

ESP/MD5/HMAC-128 = ESP protocol using HMAC (Hashed Message Authentication Coding) with the MD5 hash function using a 128-bit key. This is the default selection.

ESP/SHA/HMAC-160 = ESP protocol using HMAC with the SHA-1 hash function using a 160-bit key. This selection is more secure but requires more processing overhead.

Encryption Algorithm

This parameter specifies the data, or packet, encryption algorithm. Data encryption makes the data unreadable if intercepted.

Click the drop-down menu button and select the algorithm:

Null = No packet encryption.

DES-56 = Use DES encryption with a 56-bit key.

3DES-168 = Use Triple-DES encryption with a 168-bit key. This is the default selection, and it is the most secure.

Encapsulation Mode

This parameter specifies the mode for applying ESP encryption and authentication; in other words, what part of the original IP packet has ESP applied.

Click the drop-down menu button and select the mode:

Tunnel = Apply ESP encryption and authentication to the entire original IP packet (IP header and data), thus hiding the ultimate source and destination addresses. This is the default selection, and it is the most secure.

Transport = Apply ESP encryption and authentication only to the transport layer segment (data only) of the original IP packet. This mode protects packet contents but not the ultimate source and destination addresses. Use this mode for Windows 2000 client compatibility.

Perfect Forward Secrecy

This parameter specifies whether to use Perfect Forward Secrecy, and the size of the numbers to use, in generating Phase 2 IPsec keys. Perfect Forward Secrecy is a cryptographic concept where each new key is unrelated to any previous key. In IPsec negotiations, Phase 2 keys are based on Phase 1 keys unless Perfect Forward Secrecy is specified. Perfect Forward Secrecy uses Diffie-Hellman techniques to generate the keys.

Click the drop-down menu button and select the Perfect Forward Secrecy option:

Disabled = Don't use Perfect Forward Secrecy. IPsec Phase 2 keys are based on Phase 1 keys. This is the default selection.

Group 1 (768-bits) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 1 to generate IPsec Phase 2 keys, where the prime and generator numbers are 768 bits. This option is more secure but requires more processing overhead.

Group 2 (1024-bits) = Use Perfect Forward Secrecy, and use Diffie-Hellman Group 2 to generate IPsec Phase 2 keys, where the prime and generator numbers are 1024 bits. This option is most secure but requires the most processing overhead.

Lifetime Measurement

This parameter specifies how to measure the lifetime of the IPsec SA keys, which is how long the IPsec SA lasts until it expires and must be renegotiated with new keys. It is used with the **Data Lifetime** or **Time Lifetime** parameters below.

Click the drop-down menu button and select the measurement method:

Time = Use time (seconds) to measure the lifetime of the SA (the default). Configure the **Time Lifetime** parameter below.

Data = Use data (number of kilobytes) to measure the lifetime of the SA. Configure the **Data Lifetime** parameter below.

Both = Use both time and data, whichever occurs first, to measure the lifetime. Configure both **Time Lifetime** and **Data Lifetime** parameters.

None = No lifetime measurement. The SA lasts until the connection is terminated for other reasons.

Data Lifetime

If you select **Data** or **Both** under **Lifetime Measurement** above, enter the number of kilobytes of payload data after which the IPsec SA expires. Minimum is 100 KB, default is 10000 KB, maximum is 2147483647 KB.

Time Lifetime

If you select **Time** or **Both** under **Lifetime Measurement** above, enter the number of seconds after which the IPsec SA expires. Minimum is 60 seconds, default is 28800 seconds (8 hours), maximum is 2147483647 seconds (about 68 years).

IKE Parameters

These parameters govern IKE SAs, which are Phase 1 SAs negotiated under IPSec, where the two parties establish a secure tunnel within which they then negotiate the IPSec SAs. In this IKE SA they exchange automated key management information under the IKE (Internet Key Exchange) protocol (formerly called ISAKMP/Oakley).

All these parameters (except **IKE Peer**) must be configured the same on both parties; the **IKE Peer** entries must mirror each other. If you create multiple IPSec SAs for use between two IKE peers, the IKE SA parameters must be the same on all SAs.

For best performance and interoperability, we strongly recommend that you use the default parameters where appropriate.

IKE Peer

This parameter applies only to IPSec LAN-to-LAN configurations. It is ignored for IPSec client-to-LAN configurations.

Enter the IP address of the remote peer VPN Concentrator. Use dotted decimal notation. This must be the IP address of the public interface on the peer VPN Concentrator.

This IP address must also match the **Peer IP Address** on the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** or **Modify** screen. It must also match the **Group Name** for the LAN-to-LAN connection. When you configure the connection on the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add** screen, the Manager automatically creates a group with the **Peer IP address** as the **Group Name**. See **Configuration | User Management** for information on groups.

When you configure this parameter on the *remote* peer, enter the IP address of *this* VPN Concentrator; i.e., the entries must mirror each other.

Negotiation Mode

This parameter sets the mode for exchanging key information and setting up the SAs. It sets the mode that the initiator of the negotiation uses; the responder auto-negotiates.

Click the drop-down menu button and select the mode:

Aggressive = A faster mode using fewer packets and fewer exchanges, but which does not protect the identity of the communicating parties.

Main = A slower mode using more packets and more exchanges, but which protects the identities of the communicating parties. This mode is more secure and it is the default selection.

Digital Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under **Administration | Certificate Management**.

Click the drop-down menu button and select the option. The list shows any digital certificates that have been installed, plus:

None (Use Preshared Keys) = Use preshared keys to authenticate the peer during Phase 1 IKE negotiations. This is the default selection.

IKE Proposal

This parameter specifies the set of attributes that govern Phase 1 IPSec negotiations, which are known as IKE proposals. See the **Configuration | System | Tunneling Protocols | IPSec | IKE Proposals** screen. When the VPN Concentrator is acting as an IPSec initiator, this is the *only* IKE proposal it negotiates. As an IPSec responder, the VPN Concentrator checks all active IKE proposals in priority order, to see if it can find one that agrees with parameters in the initiator's proposed SA. You must configure, activate, and prioritize IKE proposals before configuring Security Associations.

Click the drop-down menu button and select the IKE proposal. The list shows only active IKE proposals in priority order. Cisco-supplied default active proposals are:

IKE-3DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 2 to generate SA keys. This selection is the most secure, and it is the default selection.

IKE-3DES-MD5-DH1 = Use preshared keys and MD5/HMAC-128 for authentication. Use 3DES-168 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.

IKE-DES-MD5 = Use preshared keys and MD5/HMAC-128 for authentication. Use DES-56 encryption. Use D-H Group 1 to generate SA keys. This selection is compatible with the Cisco VPN 3000 Client.

Add or Apply / Cancel

To add this Security Association to the list of configured SAs, click **Add**. Or to apply your changes to this Security Association, click **Apply**. On the **Modify** screen, any changes take effect as soon as you click **Apply**. *If this SA is being used by an active filter rule or group, changes may affect tunnel traffic.* Both actions include your entry in the active configuration. The Manager returns to the **Configuration | Policy Management | Traffic Management | Security Associations** screen. Any new SA appears at the bottom of the **IPSec SAs** list.

Reminder:

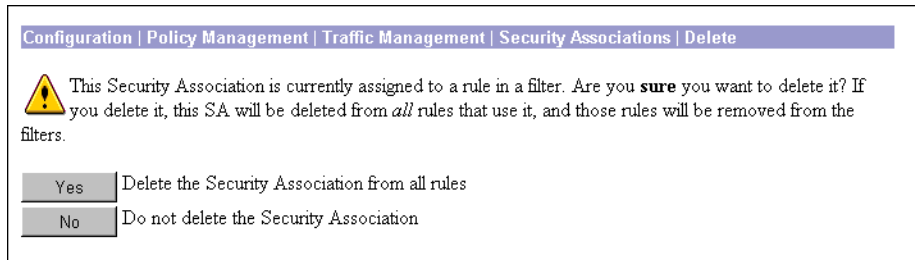
*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Security Associations** screen, and the **IPSec SAs** list is unchanged.

Configuration | Policy Management | Traffic Management | Security Associations | Delete

This screen asks you to confirm deletion of a Security Association that is assigned to a rule in a filter. *Doing so deletes the SA from the VPN Concentrator active configuration, deletes the SA from all rules that use it, and removes those rules from filters.*

Figure 13-12: Configuration | Policy Management | Traffic Management | Security Associations | Delete screen



Note: The Manager deletes the SA as soon as you click **Yes**. If this SA is being used by an active filter, deletion may affect tunnel traffic.

Yes / No

To delete this SA from all rules that use it, and delete it from the active configuration, click **Yes**. *There is no undo.* The Manager returns to the **Configuration | Policy Management | Traffic Management | Security Associations** screen and shows the remaining SAs in the **IPSec SAs** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To not delete this SA, click **No**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Security Associations** screen, and the **IPSec SAs** list is unchanged.

Configuration | Policy Management | Traffic Management | Filters

This section of the Manager lets you add, configure, modify, copy, and delete filters, and assign rules to filters.

Filters consist of rules. A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the **Action** specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the **Default Action** specified in the filter.

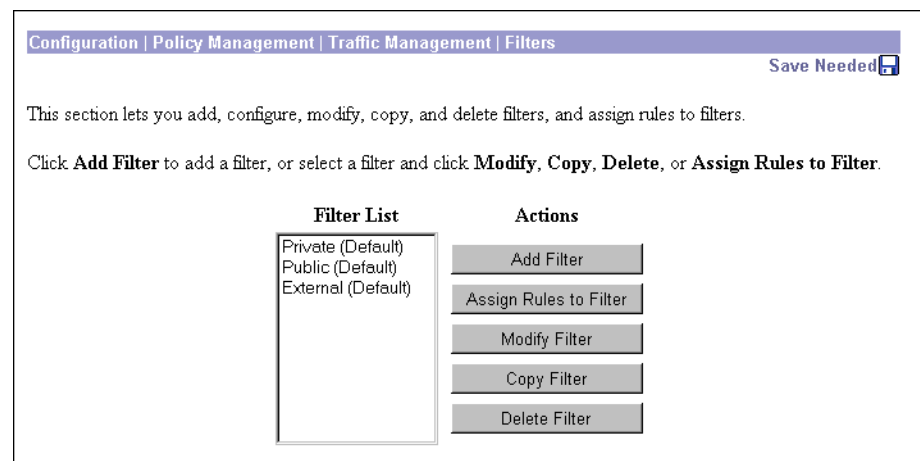
Configuring a filter involves two steps:

- 1 Configuring its basic parameters (name, default action, etc.) by clicking **Add Filter**, **Modify Filter**, or **Copy Filter**, and
- 2 Assigning rules to a filter by clicking **Assign Rules to Filter**.

You apply filters to interfaces under **Configuration | Interfaces**, and these are the most important filters for security since they govern *all* traffic through an interface. You also apply filters to groups and users under **Configuration | User Management**, and thus govern *tunneled* traffic through an interface.

Caution: The Cisco-supplied default filters and rules are intended as templates that you should examine and configure to fit your network and security needs. If incorrectly configured, they could present security risks. You should also be especially careful about adding rules to the **Public (Default)** filter, which allows only tunneled and ICMP traffic.

Figure 13-13: Configuration | Policy Management | Traffic Management | Filters screen



Filter List

The **Filter List** shows configured filters, listed in the order they are configured. Cisco supplies default filters that you can use and modify; see Table 13-3.

Table 13-3: Cisco-supplied default filters

Parameter	Private (Default)	Public (Default)	External (Default)
Description	Default filter for the Private Interface	Default filter for the Public Interface	Default filter for the External Interface
Default Action	Drop	Drop	Drop
Source Routing	No	No	No
Fragments	Yes	Yes	Yes
Current Rules in Filter	Any In (forward/in) Any Out (forward/out)	GRE In (forward/in) IPSEC-ESP In (forward/in) IKE In (forward/in) PPTP In (forward/in) L2TP In (forward/in) ICMP In (forward/in) VRRP In (forward/in) GRE Out (forward/out) IKE Out (forward/out) PPTP Out (forward/out) L2TP Out (forward/out) ICMP Out (forward/out) VRRP Out (forward/out)	-Empty-

Add Filter

To configure and add a new filter, click **Add Filter**. The Manager opens the **Configuration | Policy Management | Traffic Management | Filters | Add** screen. The Manager then automatically lets you assign rules to the filter.

Assign Rules to Filter

To assign or change rules in a configured filter, select the filter from the list and click **Assign Rules to Filter**. The Manager opens the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen, which lets you assign and order the rules that apply to this filter.

Modify Filter

To modify the basic parameters—but not the rules—for a filter that has been configured, click **Modify Filter**. The Manager opens the **Configuration | Policy Management | Traffic Management | Filters | Modify** screen.

Copy Filter

To create a new filter by copying the basic parameters and rules from a filter that has been configured, click **Copy Filter**. The Manager opens the **Configuration | Policy Management | Traffic Management | Filters | Copy** screen.

Delete Filter

To delete a configured filter, select the filter from the list and click **Delete Filter**. See notes below. The Manager refreshes the screen and shows the remaining entries in the **Filter List**.

Notes: You *cannot* delete a filter that has been applied to an interface. If you try to do so, the Manager displays an error message.

You *can* delete a filter that has been applied to a group or user, *and there is no confirmation or undo*. Doing so may affect their use of the VPN.

Reminder: *The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Filters | Add, Modify, or Copy

These screens let you:

Add: Configure the basic parameters for a new filter and add it to the list.

Modify: Modify the basic parameters for a configured filter.

Copy: Create a new filter that is a copy of a configured filter, and configure its basic parameters. The copy also includes all the rules and SAs of the original filter *except* rules with an **Apply IPSec** action.

You configure the rules in a filter on the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen.

Note: On the **Modify** screen, any changes take effect as soon as you click **Apply**. If this filter is being used by an interface or group, changes may affect data traffic.

Figure 13-14: Configuration | Policy Management | Traffic Management | Filters | Add, Modify, or Copy screen

The image shows three overlapping screenshots of a web-based configuration interface. The top screenshot is titled 'Configuration | Policy Management | Traffic Management | Filters | Copy' and contains the text 'Copy a configured filter.' The middle screenshot is titled 'Configuration | Policy Management | Traffic Management | Filters | Modify' and contains the text 'Modify a configured filter.' The bottom screenshot is titled 'Configuration | Policy Management | Traffic Management | Filters | Add' and contains the following form fields and instructions:

Configure and add a new filter.

Filter Name Name of the filter you are adding. The name must be unique.

Default Action Select the default action to take when no rules on this filter apply.

Source Routing Check to have this filter allow IP source routed packets to pass.

Fragments Check to have this filter allow fragmented IP packets to pass.

Description

Filter Name

Enter a unique name for this filter. Maximum is 48 characters.

Default Action

Click the drop-down menu button and select the action that this filter takes if a data packet *does not match* any of the rules on this filter. The choices are:

Drop = Discard the packet (the default selection).

Forward = Allow the packet to pass.

Drop and Log = Discard the packet and log a filter debugging event (FILTERDBG event class). See **Configuration | System | Events** and see note below.

Forward and Log = Allow the packet to pass and log a filter debugging event (FILTERDBG event class). See note below.

Note: The **Log** actions are intended for use only while debugging filter activity. Since they generate and log an event for every matched packet, they consume significant system resources and may seriously degrade performance.

Source Routing

Check this box to allow IP source routed packets to pass. A source routed packet specifies its own route through the network and does not rely on the system to control forwarding. This box is not checked by default, because source-routed packets can present a security risk.

Fragments

Check this box to allow fragmented IP packets to pass. Large data packets may be fragmented on their journey through networks, and the destination system reassembles them. While you would normally allow fragmented packets to pass, you might disallow them if you suspect a security problem. This box is checked by default.

Description

Enter a description of this filter. This optional field is a convenience for you or other administrators; use it to describe the purpose or use of the filter. Maximum is 255 characters.

Add or Apply / Cancel

Add screen:

To add this filter to the list of filters, click **Add**. The Manager opens the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen, which lets you assign and order the rules that apply to this filter.

Modify screen:

To apply your changes to this filter, click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Filters** screen, and the modified filter appears in same location in the **Filter List**. *Any changes take effect as soon as you click **Apply**. If this filter is being used by an active interface or group, changes may affect data traffic.*

Copy screen:

To apply your settings and add this filter to the list of filters, click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Filters** screen, and the new filter appears in the **Filter List**. To assign or change rules on the filter, select the filter from the list and click **Assign Rules to Filter**.

To discard your changes, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Filters** screen, and the **Filter List** is unchanged.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Assign Rules to Filter

This section of the Manager lets you add, remove, and prioritize the rules in a filter, and assign Security Associations to rules that are configured with an **Apply IPSec** action.

A filter applies its rules to data packets coming through the system, in the order the rules are arranged on the filter. If a rule matches, the system takes the **Action** specified in the rule. If not, it applies the next rule; and so on. If no rule matches, the system takes the **Default Action** specified in the filter.

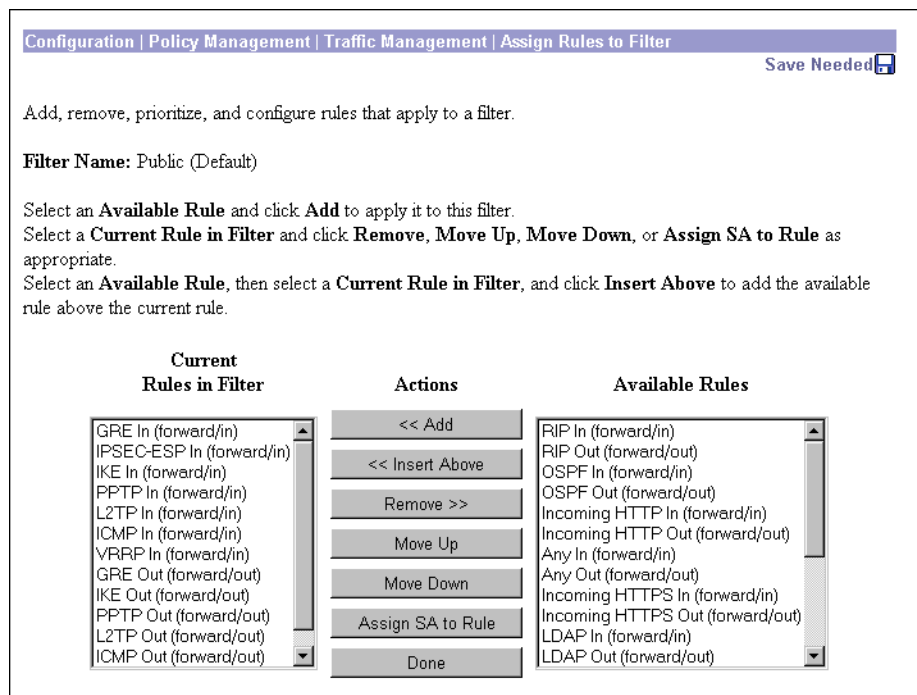
The Manager groups applied rules by direction (inbound or outbound), with inbound rules first. You can prioritize rules only within a direction.

You configure rules on the **Configuration | Policy Management | Traffic Management | Rules** screens.

Notes: Rules affect the operation of the filter as soon as you add, remove, or prioritize them. If the filter is being used by an active interface or group, changes may affect data traffic.

Be careful about adding or changing rules on the **Public (Default)** filter. You could compromise security.

Figure 13-15: Configuration | Policy Management | Traffic Management | Assign Rules to Filter screen



Filter Name:

The name of the filter whose rules you are configuring. You cannot change this name here. (See **Configuration | Policy Management | Traffic Management | Filters | Modify**.)

Current Rules in Filter

This list shows the rules currently assigned to the filter. Use the scroll controls (if present) to see all the rules in the list. If no rules have been assigned, the list shows **--Empty--**. Each entry shows the rule name and the action/direction in parentheses; **Apply IPSec** rules include their Security Association.

Available Rules

This list shows all the rules currently configured on the system (i.e., all the rules in the active configuration) that have not been assigned to this filter. Use the scroll controls (if present) to see all the rules in the list. Each entry shows the rule name and the action/direction in parentheses. (Since Security Associations are added to **Apply IPSec** rules only when those rules are assigned to a filter, this list does not show SAs.)

<< Add

To add a rule to the filter, select the rule from the **Available Rules** list and click **<< Add**. The Manager moves the rule to the **Current Rules in Filter** list, modifies the active configuration, refreshes the screen, and by default orders the current rules with all inbound rules preceding all outbound rules.

If you add a rule that has an **Apply IPSec** action configured, the Manager displays the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule** screen, which lets you add a Security Association to the rule. The Manager also, by default, adds **Apply IPSec** rules to the top of the group of rules with the same direction (inbound or outbound).

<< Insert Above

To add an available rule above a current rule, select the rule from the **Available Rules** list, then select a target rule in the **Current Rules in Filter** list, and click **Insert Above**. The Manager moves the rule to the **Current Rules in Filter** list, modifies the active configuration, refreshes the screen, and orders the new rule above the current rule. Both selected rules must have the same direction (inbound or outbound).

If you add a rule that has an **Apply IPSec** action configured, the Manager displays the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule** screen, which lets you add a Security Association to the rule.

>> Remove

To remove a rule from the filter, select the rule from the **Current Rules in Filter** list and click **>> Remove**. The Manager moves the rule to the **Available Rules** list, modifies the active configuration, refreshes the screen, and shows the remaining current rules in the filter.

You cannot remove a rule that is configured as part of a LAN-to-LAN connection. See the **Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add | Done** screen.

Move Up / Move Down

To change the order in which a rule is applied within the filter, select the rule from the **Current Rules in Filter** list and click **Move Up** or **Move Down**. The Manager reorders the current rules, modifies the active configuration, refreshes the screen, and shows the reordered list. If you try to move a rule out of its direction group (inbound or outbound), the Manager displays an error message.

Assign SA to Rule

To modify the Security Association applied to a current rule that has an **Apply IPSec** action configured, select the rule from the **Current Rules in Filter** list and click **Assign SA to Rule**. The Manager displays the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule** screen.

Done

When you are finished configuring the rules in this filter, click **Done**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Filters** screen and refreshes the **Filter List**.

Reminder:

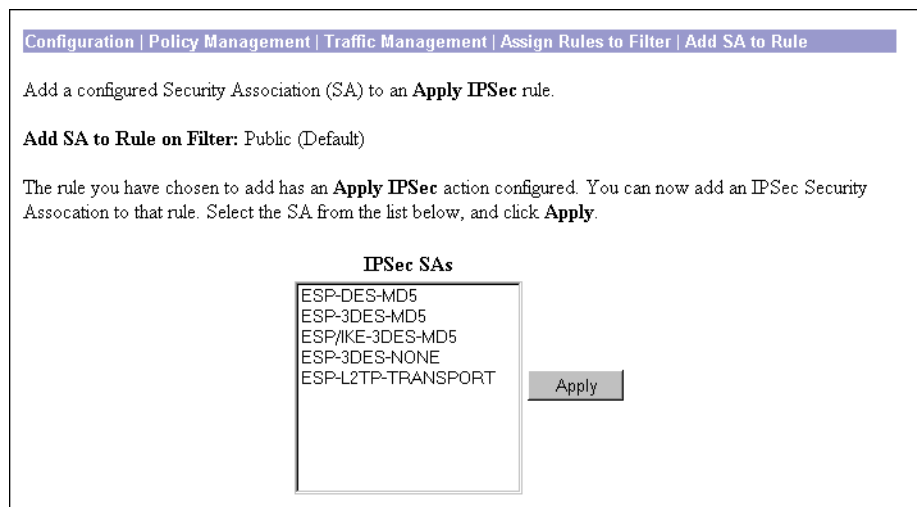
*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule

This screen lets you add a configured Security Association to a rule that has an **Apply IPSec** action configured. You can assign only one SA to a rule.

You configure Security Associations on the **Configuration | Policy Management | Traffic Management | Security Associations** screens.

Figure 13-16: Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Add SA to Rule screen



Add SA to Rule on Filter:

The Manager shows the name of filter to which you are adding a rule that has an **Apply IPSec** action configured. You cannot change this name here. See **Configuration | Policy Management | Traffic Management | Filters | Modify**.

IPSec SAs

The **IPSec SAs** list shows the configured SAs that are available; i.e., all the SAs in the active configuration.

Apply

To add an SA to the rule, select the SA from the list and click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen for the filter you are configuring, modifies the active configuration, and updates the **Current Rules in Filter** list to show the rule with its SA.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

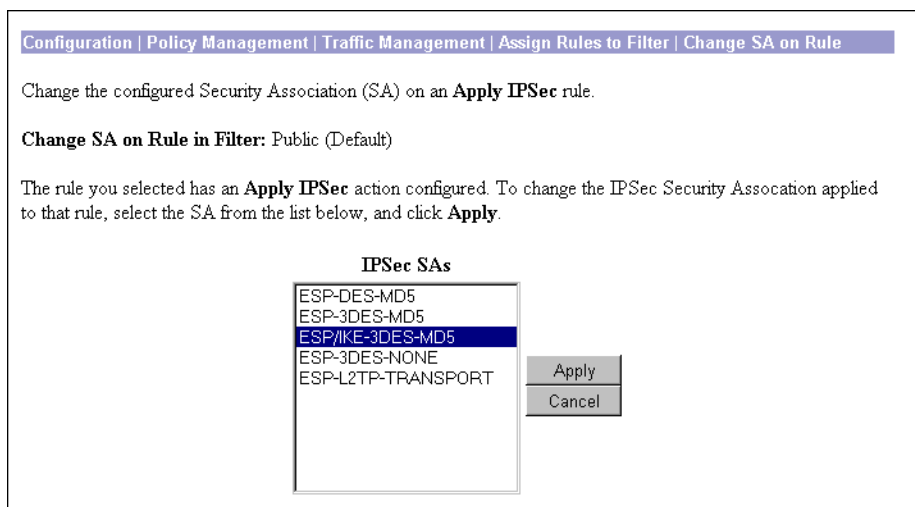
Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule

This screen lets you change the configured Security Association that is applied to a rule that has an **Apply IPSec** action configured. You can assign only one SA to a rule.

On this screen, you change *which* SA is applied. You configure SAs themselves on the **Configuration | Policy Management | Traffic Management | Security Associations** screens.

Note: The change takes effect as soon as you click **Apply**. If this filter is being used by an interface or group, the change may affect tunnel traffic.

Figure 13-17: Configuration | Policy Management | Traffic Management | Assign Rules to Filter | Change SA on Rule screen



Change SA on Rule in Filter:

The Manager shows the name of the filter to which the IPSec rule is assigned. You cannot change this name here. See **Configuration | Policy Management | Traffic Management | Filters | Modify**.

IPSec SAs

The **IPSec SAs** list shows the configured SAs that are available; i.e., all the SAs in the active configuration. By default, the SA that is currently applied to the rule is selected.

Apply / Cancel

To apply a different SA to this rule, select the SA from the list and click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen for the filter you are configuring, modifies the active configuration, and updates the **Current Rules in Filter** list to show the rule with its new SA. *The change takes effect as soon as you click **Apply**. If this filter is being used by an active interface or group, the change may affect tunnel traffic.*

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard the change and keep the current SA on the rule, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | Assign Rules to Filter** screen for the filter you are configuring, and the **Current Rules in Filter** list is unchanged.

Configuration | Policy Management | Traffic Management | NAT

This section of the Manager lets you configure and enable NAT (Network Address Translation). NAT translates private network addresses into an IANA-assigned public network address, and vice versa, and thus allows traffic routing between the networks.

The VPN Concentrator provides many-to-one translation; that is, it translates many private network addresses to the single address configured on the public network interface.

Since tunneling functions already provide NAT-like translation for tunneled data traffic, the NAT functions here provide translation for other (nontunneled) data traffic routed through the VPN Concentrator.

To use NAT, we recommend that you first configure NAT rules, then enable the function. Before you can configure NAT rules, however, you must assign an IP address to a public interface on the VPN Concentrator; see **Configuration | Interfaces**.

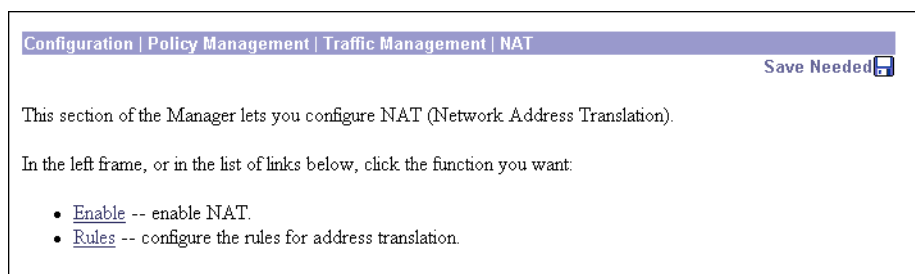
NAT examines and applies rules in this order:

- **FTP Proxy** rules
- **Map TCP**, **Map TCP/UDP**, and **Map UDP** rules
- **No Port Mapping** rules

See **Configuration | Policy Management | Traffic Management | NAT | Rules | Add** for descriptions of the rules.

You can change NAT rules while NAT is enabled. Doing so will affect subsequent sessions, but not current sessions.

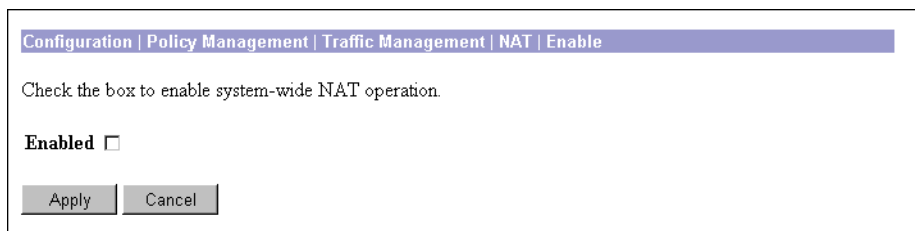
Figure 13-18: Configuration | Policy Management | Traffic Management | NAT screen



Configuration | Policy Management | Traffic Management | NAT | Enable

This screen lets you enable system-wide NAT operation, which applies NAT to all configured traffic flowing through the public interface. We recommend that you configure NAT rules before you enable the function.

Figure 13-19: Configuration | Policy Management | Traffic Management | NAT | Enable screen



Configuration | Policy Management | Traffic Management | NAT | Enable

Check the box to enable system-wide NAT operation.

Enabled

Apply Cancel

Enabled

Check the box to enable NAT, or clear it to disable NAT. By default, the box is not checked.

Apply / Cancel

To enable or disable NAT, and include your setting in the active configuration, click **Apply**. The Manager returns to the **Configuration | Policy Management | Traffic Management | NAT** screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

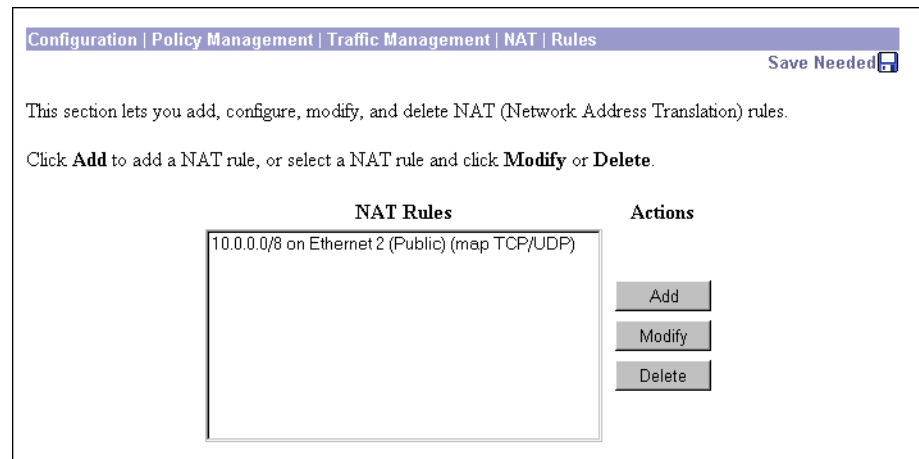
To discard your entry and leave the active configuration unchanged, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | NAT** screen.

Configuration | Policy Management | Traffic Management | NAT | Rules

This section of the Manager lets you add, configure, modify, and delete NAT rules. We recommend that you first configure and add rules, then enable the function. To configure NAT rules, you must first configure a VPN Concentrator public interface; see **Configuration | Interfaces**.

You can configure a maximum of 10 NAT rules. A typical system might have three rules:

- Provide **FTP Proxy** services for all private network addresses.
- **Map TCP/UDP** ports in packets to and from all private network addresses.
- Translate IP addresses for protocols that don't use ports (**No Port Mapping**).

Figure 13-20: Configuration | Policy Management | Traffic Management | NAT | Rules screen

NAT Rules

The **NAT Rules** list shows NAT rules that have been configured. If no rules have been configured, the list shows **--Empty--**. The format of each rule is: `Private Address/Subnet-Mask-1s on Interface (Action)`; for example, `10.0.0.0/8 on Ethernet 2 (Public) (map TCP/UDP)`.

Add / Modify / Delete

To configure and add a new NAT rule to the list of configured rules, click **Add**. The Manager opens the **Configuration | Policy Management | Traffic Management | NAT | Rules | Add** screen. If you have not configured a public interface, the Manager displays the **Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces** screen.

To modify a configured NAT rule, select the rule from the **NAT Rules** list and click **Modify**. The Manager opens the **Configuration | Policy Management | Traffic Management | NAT | Rules | Modify** screen.

To delete a configured NAT rule, select the rule from the **NAT Rules** list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining rules in the list.

Reminder:

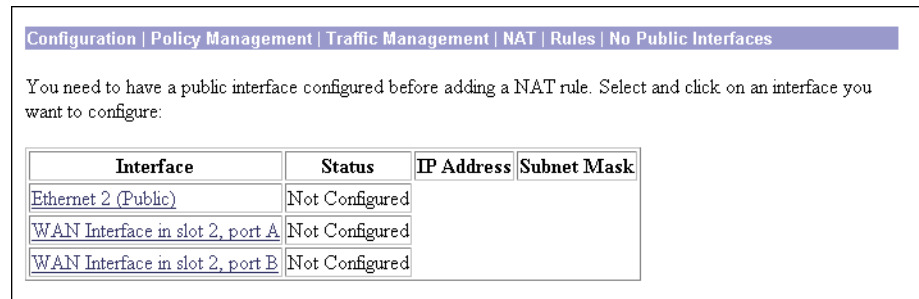
*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces

The Manager displays this screen if you have not configured a public interface on the VPN Concentrator and you try to add a NAT rule. The public interface need not be enabled, but it must be configured with an IP address and the **Public Interface** parameter enabled.

You should designate only one VPN Concentrator interface as a public interface.

Figure 13-21: Configuration | Policy Management | Traffic Management | NAT | Rules | No Public Interfaces screen



Click the highlighted link to configure the desired public interface. The Manager opens the appropriate **Configuration | Interfaces** screen.

Configuration | Policy Management | Traffic Management | NAT | Rules | Add or Modify

These screens let you:

Add: Configure and add a new NAT rule.

Modify: Modify a previously configured NAT rule.

You must configure a public interface on the VPN Concentrator before you can add a NAT rule. See the **Configuration | Interfaces** screens.

Figure 13-22: Configuration | Policy Management | Traffic Management | NAT | Rules | Add or Modify screen

The screenshot shows two overlapping windows from a configuration interface. The top window is titled 'Configuration | Policy Management | Traffic Management | NAT | Rules | Modify' and contains the text 'Modify a configured NAT rule.' The bottom window is titled 'Configuration | Policy Management | Traffic Management | NAT | Rules | Add' and contains the following fields and instructions:

- Interface:** A dropdown menu showing 'Ethernet 2 (Public) (192.168.12.34)' with the instruction 'Select the interface to put this NAT rule on.'
- Private Address:**
 - IP Address:** An empty text input field.
 - Subnet Mask:** A text input field containing '255.255.255.255'. To its right is the instruction: 'Specify the private IP address and subnet mask that this rule checks.'
- Action:** A dropdown menu showing 'No Port Mapping' with the instruction 'Select the translation action for this rule.'
- At the bottom are two buttons: 'Add' and 'Cancel'.

Interface

Add screen:

Click the drop-down menu button and select the configured public interface for this NAT rule. The list shows all interfaces (Ethernet or WAN) that have the **Public Interface** parameter enabled. See **Configuration | Interfaces**.

Modify screen:

The screen shows the configured public interface for this NAT rule. You cannot change the interface. To move the rule to another interface, you must delete this rule and add a new one for the other interface.

Private Address

Specify the private network (subnet) addresses that NAT translates to and from the public address.

IP Address

Enter the private IP address in dotted decimal notation; e.g., 10.0.0.0.

Subnet Mask

Enter the subnet mask appropriate for the private IP address range. Use dotted decimal notation; the default is 255.255.255.255. For example, to translate all private addresses in the 10. subdomain, enter 255.0.0.0.

In the **NAT Rules** list, the subnet mask is shown as the number of 1s; for example, 255.255.0.0 is shown as /16.

Action

Click the drop-down menu button and select the translation action for this NAT rule:

No Port Mapping = Translate addresses for packets with protocols that don't use ports and thus don't involve port mapping (default). For example, this action supports ping, which uses ICMP.

Map TCP/UDP = Map ports within outbound TCP and UDP packets to dynamic ports (49152 to 65535) on the public IP address, and vice versa. This is the most common type of mapping. It allows most applications, including Web browsing, to function through NAT.

Map TCP = Map ports within outbound TCP packets to dynamic ports (49152 to 65535) on the public IP address, and vice versa.

Map UDP = Map ports within outbound UDP packets to dynamic ports (49152 to 65535) on the public IP address, and vice versa.

FTP Proxy = Provide FTP proxy server functions and map outbound ports to dynamic ports (49152 to 65535) on the public IP address. FTP requires specialized NAT behavior; this action allows outgoing FTP transactions to function properly.

Add or Apply / Cancel

To add this rule to the list of configured NAT rules, click **Add**. Or to apply your changes to this NAT rule, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Configuration | Policy Management | Traffic Management | NAT | Rules** screen. Any new rule appears at the bottom of the **NAT Rules** list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the **Configuration | Policy Management | Traffic Management | NAT | Rules** screen, and the **NAT Rules** list is unchanged.

End of Chapter



Administration

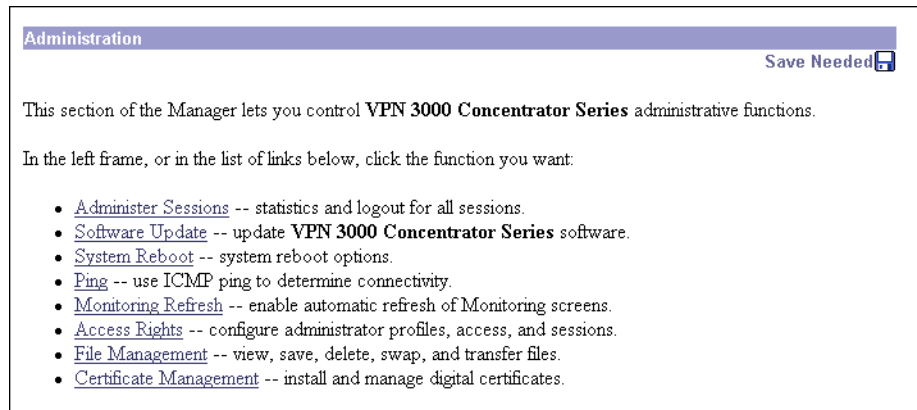
Administering the VPN 3000 Concentrator Series involves activities that keep the system operational and secure. Configuring the system sets the parameters that govern its use and functionality as a VPN device, but administration involves higher level activities such as who is allowed to configure the system, and what software runs on it. Only administrators can use the VPN Concentrator Manager.

Administration

This section of the Manager lets you control administrative functions on the VPN Concentrator.

- **Administer Sessions:** view statistics for, log out, and ping sessions.
- **Software Update:** upload and update the VPN Concentrator software image.
- **System Reboot:** set options for VPN Concentrator shutdown and reboot.
- **Ping:** use ICMP ping to determine connectivity.
- **Monitoring Refresh:** enable automatic refresh of status and statistics in the **Monitoring** section of the Manager.
- **Access Rights:** configure administrator profiles, access, and sessions.
 - **Administrators:** configure administrator usernames, passwords, and rights.
 - **Access Control List:** configure IP addresses for workstations with access rights.
 - **Access Settings:** set administrative session idle timeout and limits.
- **File Management:** manage system files in flash memory.
 - **Files:** copy, view, and delete system files.
 - **Swap Configuration Files:** swap backup and boot configuration files.
 - **TFTP Transfer:** use TFTP to transfer files to and from the VPN Concentrator.
- **Certificate Management:** install and manage digital certificates.
 - **Enrollment:** create a certificate request to send to a Certificate Authority.
 - **Installation:** install digital certificates.
 - **Certificates:** view, modify, and delete digital certificates.

Figure 14-1: Administration screen



Administration | Sessions

This screen shows comprehensive statistics for all active sessions on the VPN Concentrator.

You can also click a session's name to see detailed parameters and statistics for that session. See [Administration | Sessions | Detail](#).

Figure 14-2: Administration | Sessions screen

Administration | Sessions
Thu, 15 Jun 2000 05:06:53 PM

[Refresh](#)

This screen shows statistics for sessions.

To refresh the statistics, click **Refresh**.

For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Logout All: [PPTP](#) | [L2TP](#) | [IPSec User](#) | [L2TP/IPSec](#) | [IPSec/NAT](#) | [IPSec/LAN-to-LAN](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	2	3	6	7	1250	33

LAN-to-LAN Sessions [[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Actions
100.to 192	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	Jun 15 15:58:56	1:07:57	[Logout Ping]

Remote Access Sessions [[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Actions
user1	80.150.0.135	100.177.2.1	PPTP	RC4-128 Stateless	Jun 15 17:05:10	0:01:43	[Logout Ping]
l2tp 1	80.150.0.3	100.177.2.2	L2TP	None	Jun 15 17:05:17	0:01:36	[Logout Ping]

Management Sessions [[LAN-to-LAN Sessions](#) | [Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration	Actions
admin	Local	Console	None	Jun 15 16:59:45	0:07:08	[Logout Ping]
admin	100.200.147.1	HTTP	None	Jun 15 16:55:05	0:11:48	[Logout Ping]
admin	100.150.1.1	HTTP	None	Jun 15 16:31:04	0:35:49	[Logout Ping]

Configuration locked by 100.150.1.1

Refresh

To refresh the statistics, click **Refresh**.

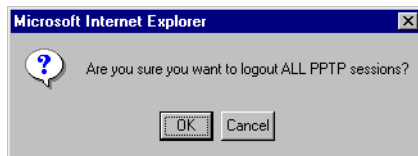
Logout All: PPTP | L2TP | IPSec User | L2TP/IPSec | IPSec/NAT | IPSec/LAN-to-LAN

These active labels let you log out *all* active sessions of a given tunnel type at once:

- **PPTP**
- **L2TP**
- **IPSec User** = IPSec remote-access users
- **L2TP/IPSec** = L2TP over IPSec
- **IPSec/NAT** = IPSec through NAT
- **IPSec/LAN-to-LAN** = IPSec LAN-to-LAN

To log out the sessions, click the appropriate label. The Manager displays a prompt to confirm the action.

Figure 14-3: Logout All Sessions confirmation prompt



Caution: This action immediately terminates *all* sessions of the given tunnel type. *There is no user warning or undo.*

The Manager refreshes the screen after it terminates the sessions.

Session Summary table

This table shows summary totals for LAN-to-LAN, remote access, and management sessions.

A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

Active LAN-to-LAN Sessions

The number of IPSec LAN-to-LAN sessions that are currently active.

Active Remote Access Sessions

The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.

Active Management Sessions

The number of administrator management sessions that are currently active.

Total Active Sessions

The total number of sessions of all types that are currently active.

Peak Concurrent Sessions

The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.

Concurrent Sessions Limit

The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent; e.g., Model 3060 = 5000 sessions.

Total Cumulative Sessions

The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

LAN-to-LAN Sessions table

This table shows parameters and statistics for all active IPSec LAN-to-LAN sessions. Each session here identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

[Remote Access Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Connection Name

The name of the IPSec LAN-to-LAN connection.

To display detailed parameters and statistics for this connection, click this name. See the **Administration | Sessions | Detail** screen.

IP Address

The IP address of the remote peer VPN Concentrator or other secure gateway that initiated this LAN-to-LAN connection.

Protocol, Encryption, Login Time, Duration, Actions

See Table 14-1 on page 14-7 for definitions of these parameters.

Remote Access Sessions table

This table shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the VPN Concentrator. Remote-access sessions include PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions.

[LAN-to-LAN Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Username

The username or login name for the session. The field shows *Authenticating...* if the remote-access client is still negotiating authentication. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

To display detailed parameters and statistics for this session, click this name. See the **Administration | Sessions | Detail** screen.

Public IP Address

The public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.

Assigned IP Address

The private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network.

Protocol, Encryption, Login Time, Duration, Actions

See Table 14-1 on page 14-7 for definitions of these parameters.

Management Sessions table


This table shows parameters and statistics for all active administrator management sessions on the VPN Concentrator.

[LAN-to-LAN Sessions | Remote Access Sessions]

Click these active links to go to the other session tables on this Manager screen.

Administrator

The administrator username or login name for the session.

The lock icon  indicates the administrator who has the configuration lock; i.e., who has the right to make changes to the active system configuration. See *Configuration locked* by below.

IP Address

The IP address of the manager workstation that is accessing the system. `Local` indicates a direct connection through the **Console** port on the system.

Protocol, Encryption, Login Time, Duration, Actions

See Table 14-1 for definitions of these parameters.

Table 14-1: Parameter definitions for Administration | Sessions screen

Parameter	Definition
Protocol	The protocol this session is using. <code>Console</code> indicates a direct connection through the Console port on the system.
Encryption	The data encryption algorithm this session is using, if any.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Actions / Logout / Ping	<p>To log out a specific session, click Logout. The screen refreshes and shows the new session statistics.</p> <p><i>Caution: Clicking Logout terminates a session without warning! There is no undo.</i></p> <p>To test the network connection to a session, click Ping. The VPN Concentrator sends an ICMP Ping message to the session IP address. See the Administration Ping screen for details and results.</p>

Configuration locked by

The administrator (IP address or `Console`) who has the right to make changes to the active system configuration.

The configuration is locked by the administrator who first makes a change to the active (running) configuration. That administrator holds the lock until logout, or until the **Session Idle Timeout** period expires (see the **Administration | Access Rights | Access Settings** screen). For example, an administrator who is just viewing and refreshing statistics on a **Monitoring** screen for longer than the timeout period, loses the lock.

Administration | Sessions | Detail

These Manager screens show detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. There are unique screens for:

- IPSec LAN-to-LAN (IPSec/LAN-to-LAN)
- IPSec remote access (IPSec User)
- IPSec through NAT (IPSec/NAT)
- L2TP
- L2TP over IPSec (L2TP/IPSec)
- PPTP

The Manager displays the appropriate screen when you click a highlighted connection name or username on the **Administration | Sessions** screen. See Figure 14-4 through Figure 14-9 below.

Each session detail screen shows two tables: summary data at the top, and detail data below. The summary data echoes the session data from the **Administration | Sessions** screen. The session detail table shows all the relevant parameters for each session and subsession.

See Table 14-2 on page 14-12 for definitions of the session detail parameters, in alphabetical order.

Figure 14-4: Administration | Sessions | Detail screen: IPSec LAN-to-LAN

Administration | Sessions | Detail
Thu, 15 Jun 2000 05:07:37 PM

[Refresh](#)

[Back to Sessions](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
100.to.192	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	Jun 15 15:58:56	1:08:41	9744	19136

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	192.168.84.0/0.0.0.255
Local Address	100.0.0.0/0.255.255.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Bytes Received	19136	Bytes Transmitted	9744

Figure 14-5: Administration | Sessions | Detail screen: IPSec remote access user

Administration | Sessions | Detail
Thu, 15 Jun 2000 05:13:22 PM

[Refresh](#)

[Back to Sessions](#)

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
client	80.150.0.1	100.177.2.4	IPSec	3DES-168	Jun 15 17:11:23	0:01:59	0	0

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Aggressive

IPSec Session			
Session ID	2	Remote Address	100.177.2.4
Local Address	200.70.50.7	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Idle Time	0:01:59	Encapsulation Mode	Tunnel
Bytes Received	0	Bytes Transmitted	0

Figure 14-6: Administration | Sessions | Detail screen: IPSec through NAT

Administration Sessions Detail		Thu, 15 Jun 2000 05:12:51 PM						
		Refresh						
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
client2	80.177.1.3	100.177.2.3	IPSec/NAT	3DES-168	Jun 15 17:10:53	0:01:58	864	600
IKE Session								
Session ID	1		Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5		Diffie-Hellman Group	Group 1 (768-bit)				
Authentication Mode	Pre-Shared Keys		IKE Negotiation Mode	Aggressive				
IPSec/NAT Session								
Session ID	2		Remote Address	100.177.2.3				
Local Address	200.70.50.7		Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5		SEP	1				
Idle Time	0:00:52		Encapsulation Mode	Tunnel				
UDP Port	33333							
Bytes Received	120		Bytes Transmitted	120				
IPSec/NAT Session								
Session ID	3		Remote Address	100.177.2.3				
Local Address	100.0.0.0/0.255.255.255		Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5		SEP	1				
Idle Time	0:01:51		Encapsulation Mode	Tunnel				
UDP Port	33333							
Bytes Received	480		Bytes Transmitted	744				

Figure 14-7: Administration | Sessions | Detail screen: L2TP

Administration Sessions Detail		Thu, 15 Jun 2000 05:06:27 PM						
		Refresh						
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
l2tp1	80.150.0.3	100.177.2.2	L2TP	None	Jun 15 17:05:17	0:01:10	242	6430
L2TP Sessions: 1								
L2TP Session								
Session ID	1		Username	l2tp1				
Assigned IP Address	100.177.2.2		Encryption Algorithm	None				
Authentication Mode	MS-CHAP v1							
Bytes Received	6430		Bytes Transmitted	242				

Figure 14-8: Administration | Sessions | Detail screen: L2TP over IPSec

Administration | Sessions | Detail Thu, 15 Jun 2000 05:13:50 PM
Refresh

[Back to Sessions](#)

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
dellauser	200.70.50.134	100.177.2.5	L2TP/IPSec	3DES-168	Jun 15 17:12:50	0:01:00	1328	12768

IKE Sessions: 1
IPSec Sessions: 1
L2TP Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Authentication Mode	RSA Certificate	IKE Negotiation Mode	Main
Rekey Time Interval	28800 seconds		

IPSec Session			
Session ID	2	Remote Address	200.70.50.134
Local Address	200.70.50.7	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Idle Time	0:00:27	Encapsulation Mode	Transport
Rekey Time Interval	3600 seconds	Rekey Data Interval	250000 KBytes
Bytes Received	12768	Bytes Transmitted	1328

L2TP/IPSec Session			
Session ID	3	Username	dellauser
Assigned IP Address	100.177.2.5	Encryption Algorithm	None
Idle Time	0:00:27	Authentication Mode	MS-CHAP v1
Bytes Received	6795	Bytes Transmitted	0

Figure 14-9: Administration | Sessions | Detail screen: PPTP

Administration | Sessions | Detail Thu, 15 Jun 2000 05:05:44 PM
Refresh

[Back to Sessions](#)

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
user1	80.150.0.135	100.177.2.1	PPTP	RC4-128 Stateless	Jun 15 17:05:09	0:00:35	0	1968

PPTP Sessions: 1

PPTP Session			
Session ID	1	Username	user1
Assigned IP Address	100.177.2.1	Encryption Algorithm	RC4-128 Stateless
Authentication Mode	MS-CHAP v1		
Bytes Received	1968	Bytes Transmitted	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back to Sessions

To return to the **Administration | Sessions** screen, click **Back to Sessions**.

Administration | Sessions | Detail parameters

Table 14-2: Parameter definitions for Administration | Sessions | Detail screens

Parameter	Definition
Assigned IP Address	The private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network.
Authentication Mode	The protocol or mode used to authenticate this session.
Bytes Rx Bytes Received	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Bytes Tx Bytes Transmitted	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Connection Name	The name of the IPSec LAN-to-LAN connection.
Diffie-Hellman Group	The algorithm and key size used to generate IPSec SA encryption keys.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Encapsulation Mode	The mode for applying IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication; i.e., what part of the original IP packet has ESP applied.
Encryption Encryption Algorithm	The data encryption algorithm this session is using, if any.
Hashing Algorithm	The algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Idle Time	The elapsed time (HH:MM:SS) between the last communication activity on this session and the last screen refresh.
IKE Negotiation Mode	The IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions:	The total number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
IP Address	The IP address of the remote peer VPN Concentrator or other secure gateway that initiated the IPSec LAN-to-LAN connection.

Table 14-2: Parameter definitions for Administration | Sessions | Detail screens (continued)

Parameter	Definition
IPSec Sessions:	The total number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session may have two IPSec sessions: one showing the tunnel endpoints, and one showing the private networks reachable through the tunnel.
L2TP Sessions:	The total number of user sessions through this L2TP or L2TP / IPSec tunnel; usually 1.
Local Address	The IP address (and wildcard mask) of the destination host (or network) for this session.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Perfect Forward Secrecy Group	The Diffie-Hellman algorithm and key size used to generate IPSec SA encryption keys using Perfect Forward Secrecy.
PPTP Sessions:	The total number of user sessions through this PPTP tunnel; usually 1.
Protocol	The tunneling protocol that this session is using.
Public IP Address	The public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
Rekey Data Interval	The lifetime in kilobytes of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	The lifetime in seconds of the IPSec (IKE) SA encryption keys.
Remote Address	The IP address (and wildcard mask) of the remote peer (or network) that initiated this session.
SEP	The Scalable Encryption Module that is handling cryptographic processing for this session.
Session ID	An identifier for session components (subsessions) on this screen. With IPSec, there is one identifier for each SA.
UDP Port	The UDP port number used in an IPSec through NAT connection.
Username	The username or login name for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

Administration | Software Update

This screen lets you update the VPN Concentrator executable system software (the software image). This process uploads the file to the VPN Concentrator, which then verifies the integrity of the file.

The new image file must be accessible by the workstation you are using to manage the VPN Concentrator. Software image files ship on the Cisco VPN 3000 Concentrator CD-ROM. Updated or patched versions are available from the Cisco Website, www.cisco.com, under **Service & Support > Software Center**.

It takes a few minutes to upload and verify the software, and the system displays the progress. Please wait for the operation to finish.

To run the new software image, you must reboot the VPN Concentrator. The system prompts you to reboot when the update is finished.

We also recommend that you clear your browser's cache after you update the software image: delete all the browser's temporary internet files, history files, and location bar references.

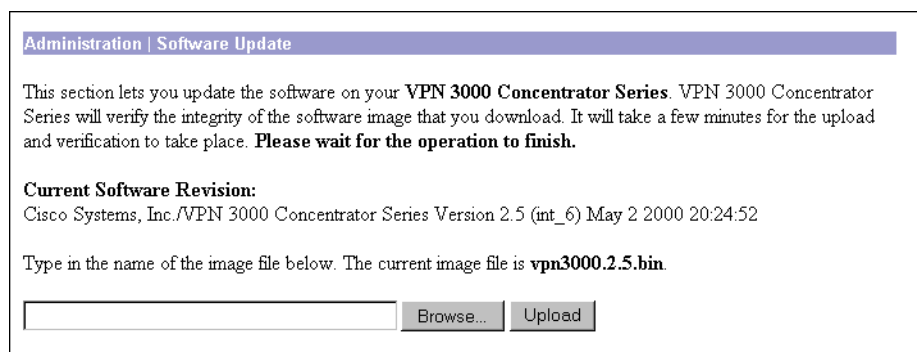
Note: The VPN Concentrator has two locations for storing image files: the active location, which stores the image currently running on the system; and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. Updating *twice*, therefore, overwrites the image file in the active location; and the current image file is lost.

Caution: You can *update* the software image while the system is still operating as a VPN device. *Rebooting* the system, however, terminates all active sessions.

While the system is updating the image, do not perform any other operations that affect flash memory (listing, viewing, copying, deleting, or writing files.) Doing so may corrupt memory.

Updating the software image also makes available any new Cisco-supplied configurable selections for filter rules, Security Associations, IKE proposals, base-group attributes, etc. When you reboot with the new image, the system updates the active configuration in memory with these new selections, but it does not write them to the CONFIG file until you click the **Save Needed** icon in the Manager window. See **Administration | File Management** for ways to manage CONFIG files.

Figure 14-10: Administration | Software Update screen



Current Software Revision

The name, version number, and date of the software image currently running on the system.

Browse...

Enter the complete pathname of the new image file, or click **Browse...** to find and select the file from your workstation or network. Cisco-supplied VPN 3000 Concentrator software image files are named:

Model 3005 = vpn3005.<Major Version>.<Minor Version>.<Patch Version>.bin;
e.g., vpn3005.2.5.bin.

Models 3015, 3030, 3060, and 3080 = vpn3000.<Major Version>.<Minor Version>.<Patch Version>.bin; e.g., vpn3000.2.5.bin.

The Major and Minor Version numbers are always present; the Patch Version number is present only if needed.

Be sure you select the correct file for your VPN Concentrator model; otherwise the update will fail.

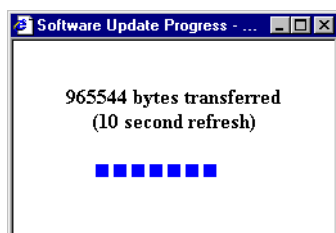
Upload

To upload the new image file to the VPN Concentrator, click **Upload**.

Software Update Progress

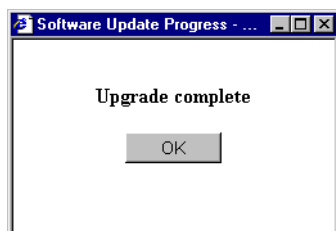
This window shows the progress of the software upload. The number of bytes transferred is refreshed in 10-second intervals.

Figure 14-11: Administration | Software Update Progress window



When the upload is finished, the system verifies the integrity of the software, and the progress window displays a completion message.

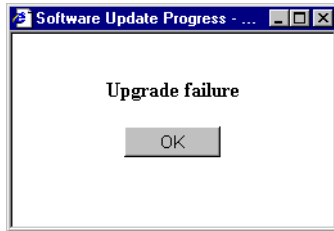
Figure 14-12: Administration | Software Update Complete window



Click **OK** to close the progress window.

If the upload or verification is not successful, the progress window displays a failure message.

Figure 14-13: Administration | Software Update Failure window



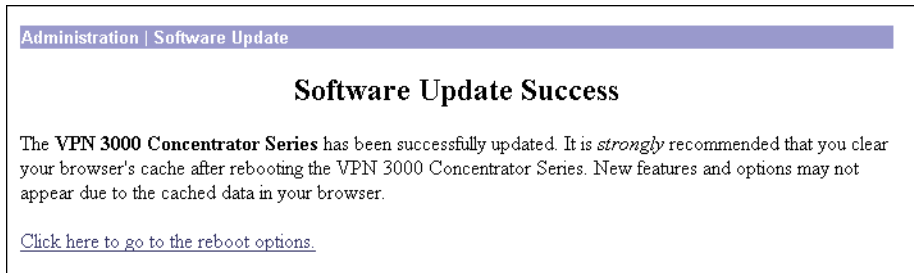
Click **OK** to close the progress window. Try the upload again.

Software Update Success

This window confirms that the software upload and verification completed successfully. To go to the **Administration | System Reboot** screen, click the highlighted link.

We strongly recommend that you clear your browser's cache after you update the software image: delete all the browser's temporary internet files, history files, and location bar references.

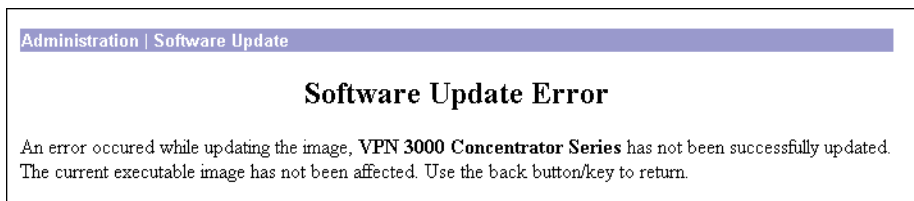
Figure 14-14: Administration | Software Update Success screen



Software Update Error

This window appears if there was an error in uploading or verifying the image file. You may have selected the wrong file. Try the update again, or contact Cisco support.

Figure 14-15: Administration | Software Update Error screen



Administration | System Reboot

This screen lets you reboot or shutdown (halt) the VPN Concentrator with various options.

We strongly recommend that you shut down the VPN Concentrator before you turn power off. If you just turn power off without shutting down, you may corrupt flash memory and affect subsequent operation of the system.

If you are logged in the Manager when the system reboots or halts, it automatically logs you out and displays the main login screen. The browser may appear to hang during a reboot; that is, you cannot log in and you must wait for the reboot to finish. You can log back in while the VPN Concentrator is in a shutdown state, before you turn power off. On the Models 3015–3080, all 10 blue usage monitor LEDs on the VPN Concentrator front panel blink when the system is in a shutdown state. On the Model 3005, the **System** LED blinks.

If a delayed reboot or shutdown is pending, the Manager also displays a message that describes when the action is scheduled to occur.

Caution: Reboot or shutdown that does not wait for sessions to terminate, terminates all active sessions without warning and prevents new user sessions.

The VPN Concentrator automatically saves the current event log file as SAVELOG.TXT when it reboots, and it overwrites any existing file with that name. See **Configuration | System | Events | General**, **Administration | File Management**, and **Monitor | Event Log** for more information on the event log file.

Figure 14-16: Administration | System Reboot screen

Administration | System Reboot
Save Needed

This section presents reboot options.

If you reboot, the browser may appear to hang as the device is rebooted.

Action

Reboot

Shutdown without automatic reboot

Cancel a scheduled reboot/shutdown

Configuration

Save the active configuration at time of reboot

Reboot without saving the active configuration

Reboot with Factory/Default configuration

When to Reboot/Shutdown

Now

Delayed by minutes

At time (24 hour clock)

Wait for sessions to terminate (don't allow new sessions)

Apply
Cancel

Action

Click a radio button to select the desired action. You can select only one action.

Reboot = Reboot the VPN Concentrator. Rebooting terminates all sessions, resets the hardware, loads and verifies the software image, executes system diagnostics, and initializes the system. A reboot takes about 60-75 seconds. (This is the default selection.)

Shutdown without automatic reboot = Shut down the VPN Concentrator; that is, bring the system to a halt so you can turn off the power. Shutdown terminates all sessions and prevents new user sessions (but not administrator sessions). While the system is in a shutdown state, the **System LED** (Model 3005) or the blue usage LEDs (Models 3015–3080) blink on the front panel.

Cancel a scheduled reboot/shutdown = Cancel a reboot or shutdown that is waiting for a certain time or for sessions to terminate. (This is the default selection if a reboot or shutdown is pending.)

Configuration

Click a radio button to select the configuration file handling at reboot. These selections apply to reboot only. You can select only one option.

Save the active configuration at time of reboot = Save the active configuration to the CONFIG file, and reboot using that new file.

Reboot without saving the active configuration = Reboot using the existing CONFIG file and without saving the active configuration. (This is the default selection.)

Reboot with Factory/Default configuration = Reboot using all the factory defaults; i.e., start the system as if it had no CONFIG file. You will need to go through all the Quick Configuration steps described in the *VPN Concentrator Getting Started* manual, including setting the system date and time and supplying an IP address for the Ethernet 1 (Private) interface, using the system console. This option *does not* destroy any existing CONFIG file, and it *does not* reset Administrator parameter settings.

When to Reboot/Shutdown

Click a radio button to select when to reboot or shutdown. You can select only one option.

Now = Reboot or shutdown as soon as you click **Apply**. (This is the default selection.)

Delayed by [NN] minutes = Reboot or shutdown NN minutes from when you click **Apply**, based on system time. Enter the desired number in the field; the default is 10 minutes. (FYI: 1440 minutes = 24 hours.)

At time [HH:MM] = Reboot or shutdown at the specified system time, based on a 24-hour clock. Enter the desired time in the field. Use 24-hour notation and enter numbers in all positions. The default is 10 minutes after the current system time.

Wait for sessions to terminate (don't allow new sessions) = Reboot or shutdown as soon as the last session terminates, and don't allow any new sessions in the meantime. If you (the administrator) are the last session, you must log out for the system to reboot or shutdown.

Apply / Cancel

To take action with the selected options, click **Apply**. The Manager returns to the main **Administration** screen if you don't reboot or shutdown now.

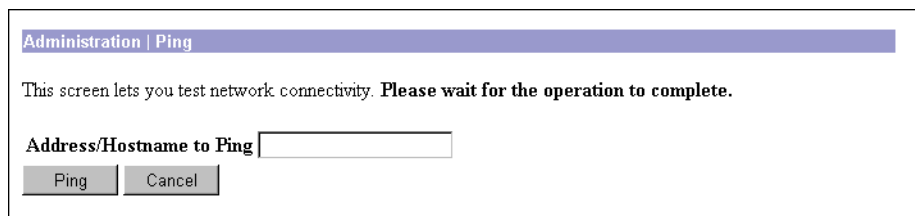
To cancel your settings on this screen, click **Cancel**. The Manager returns to the main **Administration** screen. (Note that this **Cancel** button does not cancel a scheduled reboot or shutdown.)

Administration | Ping

This screen lets you use the ICMP ping (Packet Internet Groper) utility to test network connectivity. Specifically, the VPN Concentrator sends an ICMP Echo Request message to a designated host. If the host is reachable, it returns an Echo Reply message, and the Manager displays a **Success** screen. If the host is not reachable, the Manager displays an **Error** screen.

You can also **Ping** hosts from the **Administration | Sessions** screen.

Figure 14-17: Administration | Ping screen



Administration | Ping

This screen lets you test network connectivity. Please wait for the operation to complete.

Address/Hostname to Ping

Ping Cancel

Address/Hostname to Ping

Enter the IP address or hostname of the system you want to test. (If you configured a DNS server, you can enter a hostname; otherwise, enter an IP address.) Maximum is 64 characters.

Ping / Cancel

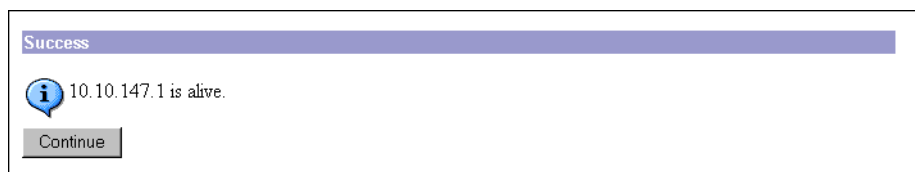
To send the ping message, click **Ping**. The Manager pauses during the test, which may take a few moments; *please wait for the operation to finish*. The Manager then displays either a **Success** or **Error** screen; see below.

To cancel your entry on this screen, click **Cancel**. The Manager returns to the main **Administration** screen.


Success (Ping)

If the system is reachable, the Manager displays a **Success** screen with the name of the tested host.

Figure 14-18: Administration | Ping | Success screen



Success

 10.10.147.1 is alive.

Continue

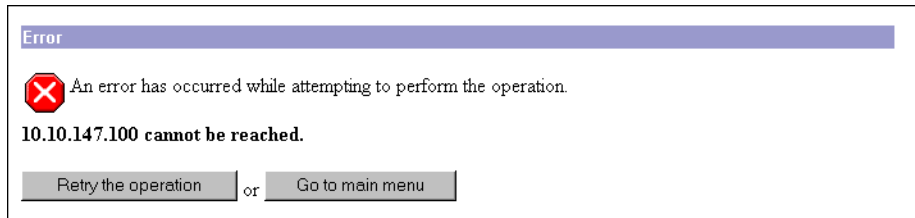
Continue

To return to the **Administration | Ping** screen, click **Continue**.

Error (Ping)

If the system is unreachable for any reason—host down, ICMP not running on host, route not configured, intermediate router down, network down or congested, etc.—the Manager displays an **Error** screen with the name of the tested host. To troubleshoot the connection, try to **Ping** other hosts that you know are working.

Figure 14-19: Administration | Ping | Error screen



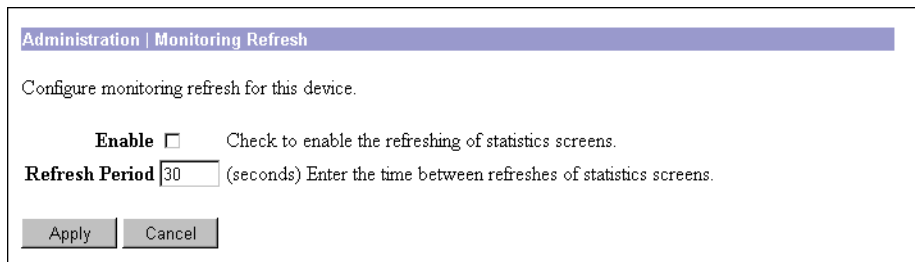
To return to the **Administration | Ping** screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

Administration | Monitoring Refresh

This screen lets you enable automatic refresh of all status and statistics screens in the **Monitoring** section of the VPN Concentrator Manager except the **Event Log**.

Figure 14-20: Administration | Monitoring Refresh screen



Enable

To enable automatic refresh, check this box. The box is not checked by default.

Refresh Period

Enter the refresh period in seconds. Minimum is 1, default is 30, and maximum is 2000000000 seconds (about 63 years). Very short periods may affect system performance.

The refresh period timer begins *after* the Manager fully displays a given screen.

Apply / Cancel

To save your settings in the active configuration, click **Apply**. The Manager goes to the main **Administration** screen.

Reminder: To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

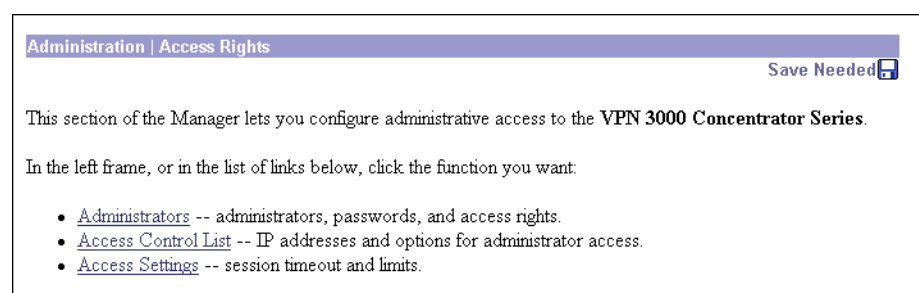
To discard your settings, click **Cancel**. The Manager goes to the main **Administration** screen.

Administration | Access Rights

This section of the Manager lets you configure and control administrative access to the VPN Concentrator.

- **Administrators:** configure administrator usernames, passwords, and rights.
- **Access Control List:** configure IP addresses for workstations with access rights.
- **Access Settings:** set administrative session timeout and limits.

Figure 14-21: Administration | Access Rights screen



Administration | Access Rights | Administrators

Administrators are special users who can access and change the configuration, administration, and monitoring functions on the VPN Concentrator. Only administrators can use the VPN Concentrator Manager.

Cisco provides five predefined administrators:

- **1 - admin** = System administrator with access to, and rights to change, all areas. This is the only administrator enabled by default; i.e., this is the only administrator who can log in to, and use, the VPN Concentrator Manager as supplied by Cisco.
- **2 - config** = Configuration administrator with all rights except SNMP access.
- **3 - isp** = Internet service provider administrator with limited general configuration rights.
- **4 - mis** = Management information systems administrator with the same rights as **config**.
- **5 - user** = User administrator with rights only to view system statistics.

This section of the Manager lets you change administrator properties and rights. Any changes take effect as soon as you click **Apply**.

Note: The VPN Concentrator saves Administrator parameter settings from this screen and the **Modify Properties** screen in nonvolatile memory, not in the active configuration (CONFIG) file. Thus, these settings are retained even if the system loses power. These settings are also retained even if you reboot the system with the factory configuration file.

Figure 14-22: Administration | Access Rights | Administrators screen

Administration | Access Rights | Administrators

This section presents administrator users. Any changes you make take effect immediately.

Group Number	Username	Properties	Administrator Enabled
1	admin	Modify	<input checked="" type="checkbox"/>
2	config	Modify	<input type="checkbox"/>
3	isp	Modify	<input type="checkbox"/>
4	mis	Modify	<input type="checkbox"/>
5	user	Modify	<input type="checkbox"/>

Apply Cancel

Group Number

This is a reference number for the administrator. Cisco assigns these numbers so you can refer to administrators by groups of properties. The numbers cannot be changed.

Username

The username, or login name, of the administrator. You can change this name on the **Administration | Access Rights | Administrators | Modify Properties** screen.

Note: *The default passwords that Cisco supplies are the same as the usernames. We strongly recommend that you change these passwords.*

Properties / Modify

To modify the username, password, and access rights of the administrator, click **Modify**. See the **Administration | Access Rights | Administrators | Modify Properties** screen.

Administrator

To assign “system administrator” privileges to one administrator, click the radio button. Only the “system administrator” can access and configure properties in this section. You can select only one. By default, **admin** is selected.

Enabled

Check the box to enable, or clear the box to disable, an administrator. Only enabled administrators can log in to, and use, the VPN Concentrator Manager. You must enable at least one administrator, and you can enable all administrators. By default, only **admin** is enabled.

Apply / Cancel

To save this screen’s settings in nonvolatile memory, click **Apply**. The settings immediately affect new sessions. The Manager returns to the **Administration | Access Rights** screen.

To discard your settings or changes, click **Cancel**. The Manager returns to the **Administration | Access Rights** screen.

Administration | Access Rights | Administrators | Modify Properties

This screen lets you modify the username, password, and rights for an administrator. Any changes affect new sessions as soon as you click **Apply** or **Default**.

Figure 14-23: Administration | Access Rights | Administrators | Modify Properties screen

Administration | Access Rights | Administrators | Modify Properties

This section lets you modify the properties for administrators. Any changes you make take effect immediately.

Username

Password A password is required.

Verify The password must be verified.

Access Rights

Authentication

General

SNMP

Files Includes Configuration Files

Table 14-3 shows the matrix of Cisco-supplied default rights for the five administrators.

Table 14-3: Cisco-supplied default administrator rights

Administrator	Authentication	General	SNMP	Files
1 - admin	Modify Config	Modify Config	Modify Config	Read/Write Files
2 - config	Modify Config	Modify Config	Stats Only	Read/Write Files
3 - isp	Stats Only	Modify Config	Stats Only	Read Files
4 - mis	Modify Config	Modify Config	Stats Only	Read Files
5 - user	Stats Only	Stats Only	Stats Only	Read Files

Username

Enter or edit the unique username for this administrator. Maximum is 31 characters.

Password

Enter or edit the unique password for this administrator. Maximum is 31 characters. The field displays only asterisks.

Note: *The default password that Cisco supplies is the same as the username. We strongly recommend that you change this password.*

Verify

Re-enter the password to verify it. The field displays only asterisks.

Access Rights

The **Access Rights** determine access to and rights in VPN Concentrator Manager functional areas (**Authentication** or **General**), or via **SNMP**. Click the drop-down menu button and select the access rights:

None = No access or rights.

Stats Only = Access to only the **Monitoring** section of the VPN Concentrator Manager. No rights to change parameters.

View Config = Access to permitted functional areas of the VPN Concentrator Manager, but no rights to change parameters.

Modify Config = Access to permitted functional areas of the VPN Concentrator Manager, and rights to change parameters.

Authentication

This area consists of VPN Concentrator Manager functions that affect authentication:

- **Configuration | User Management**
- **Configuration | Policy Management | Access Hours**
- **Configuration | Policy Management | Traffic Management | Filters**
- **Configuration | System | Servers | Authentication and Accounting.**

General

This area consists of all VPN Concentrator Manager functions except authentication and administration. (The **Administrator** radio button on the **Administration | Access Rights | Administrators** screen controls access to administration functions.)

SNMP

This parameter governs limited changes to the VPN Concentrator Manager via SNMP, using a network management system. In other words, it determines what the administrator can do via SNMP.

Files

This parameter governs rights to access and manage files in VPN Concentrator flash memory, and to save the active configuration in a file. (Flash memory acts like a disk.) Click the drop-down menu button and select the file management rights:

None = No file access or management rights.

List Files = See a list of files in VPN Concentrator flash memory.

Read Files = Read (view) files in flash memory.

Read/Write Files = Read and write files in flash memory, clear or save the event log, and save the active configuration to a file.

Apply / Default / Cancel

To save your settings in nonvolatile memory, click **Apply**. The settings take effect immediately. The Manager returns to the **Administration | Access Rights | Administrators** screen.

To restore the Cisco-supplied access rights for this administrator, and to save your settings in nonvolatile memory, click **Default**. The settings take effect immediately. *This action does not restore the default username or password.* The Manager returns to the **Administration | Access Rights | Administrators** screen.

To discard your changes, click **Cancel**. The Manager returns to the **Administration | Access Rights | Administrators** screen.

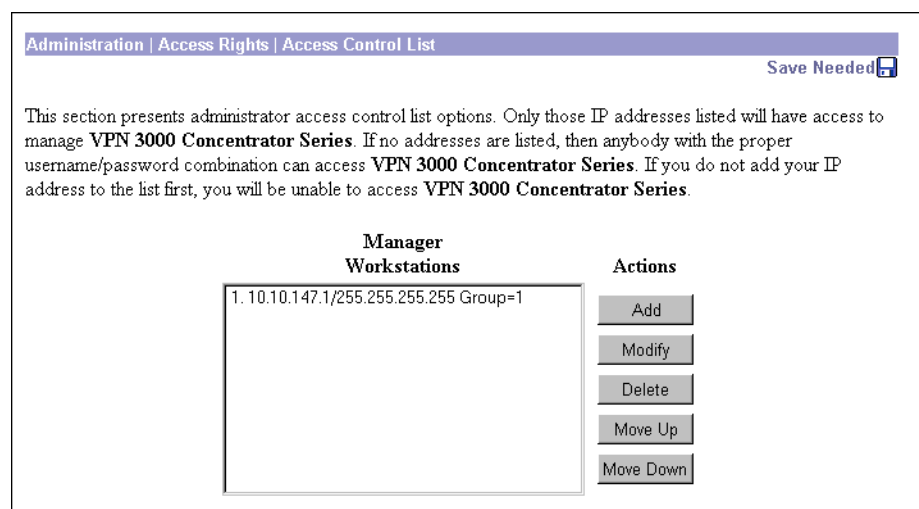
Administration | Access Rights | Access Control List

This section of the Manager lets you configure and prioritize the systems (workstations) that are allowed to access the VPN Concentrator Manager. For example, you might want to allow access only from one or two PCs that are in a locked room. If no systems are listed, then anyone who knows the VPN Concentrator IP address and the administrator username/password combination can gain access.

As soon as you add a workstation to the list, access control becomes effective for new sessions. Therefore, the first entry on the list should be the IP address of the workstation you are now using to configure the VPN Concentrator. Otherwise, if you log out or time out, you will not be able to access the Manager from the workstation.

These entries govern administrator access and management by any remote means: HTTP, FTP, TFTP, SNMP, Telnet, etc.

Figure 14-24: Administration | Access Rights | Access Control List screen



Manager Workstations

The **Manager Workstations** list shows the configured workstations that are allowed to access the VPN Concentrator Manager, in priority order. Each entry shows the priority number, IP address/ mask, and administrator group number; e.g., 1. 10.10.1.35/255.255.255.255 Group=1. If no workstations have been configured, the list shows **--Empty--**.

Add / Modify / Delete / Move

To configure a new manager workstation, click **Add**. The Manager opens the **Administration | Access Rights | Access Control List | Add** screen.

To modify a configured manager workstation, select the entry from the list and click **Modify**. The Manager opens the **Administration | Access Rights | Access Control List | Modify** screen.

To remove a configured manager workstation, select the entry from the list and click **Delete**. The Manager refreshes the screen and shows the remaining entries in the **Manager Workstations** list.

To change the priority order for configured manager workstations, select the entry from the list and click **Move ↑** or **Move ↓**. The Manager refreshes the screen and shows the reordered **Manager Workstations** list.

Reminder: The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

Administration | Access Rights | Access Control List | Add or Modify

These screens let you:

Add a manager workstation to the list of those that are allowed to access the VPN Concentrator Manager.

Modify a previously configured workstation that is allowed to access the VPN Concentrator Manager.

Figure 14-25: Administration | Access Rights | Access Control List | Add or Modify screen

Administration | Access Rights | Access Control List | Modify

Modify an administration address in the access list.

Administration | Access Rights | Access Control List | Add

Add a manager address to the access list.

IP Address

IP Mask The mask specifies the part of the address to match. Use 255.255.255.255 to match the whole address. Use 0.0.0.0 to match any address.

Access Group

- Group 1 (admin)
- Group 2 (config)
- Group 3 (isp)
- Group 4 (mis)
- Group 5 (user)
- No Access

Priority (Modify screen only)

This field shows the priority number of this workstation in the list of **Manager Workstations**. You cannot edit this field. To change the priority, use the **Move** buttons on the **Administration | Access Rights | Access Control List** screen.

IP Address

Enter the IP address of the workstation in dotted decimal notation; e.g., 10.10.1.35.

IP Mask

Enter the mask for the IP address in dotted decimal notation. This mask lets you restrict access to a single IP address, a range of addresses, or all addresses. To restrict access to a single IP address, enter 255.255.255.255 (the default). To allow all IP addresses, enter 0.0.0.0. To allow a range of IP addresses, enter the appropriate mask. For example, to allow IP addresses 10.10.1.32 through 10.10.1.35, enter the mask 255.255.255.252.

Access Group

To assign rights of an administrator group to this IP address, click the appropriate radio button. Default is **Group 1 (admin)**. You can assign only one group, or you can specify **No Access**.

Add or Apply / Cancel

To add this workstation to the list, click **Add**. Or to apply your changes to this workstation, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the **Administration | Access Rights | Access Control List** screen. Any new entry appears at the bottom of the **Manager Workstations** list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the **Administration | Access Rights | Access Control List** screen, and the **Manager Workstations** list is unchanged.

Administration | Access Rights | Access Settings

This screen lets you configure general options for administrator access to the VPN Concentrator Manager.

Figure 14-26: Administration | Access Rights | Access Settings screen

Administration | Access Rights | Access Settings

This section presents General Access options.

Session Idle Timeout (seconds) Enter the administrative session idle timeout. Limit is 1800 seconds.

Session Limit Enter the maximum number of administrative sessions.

Encrypt Config File Check to enable configuration file encryption.

Session Idle Timeout

Enter the idle timeout period in seconds for administrative sessions. If there is no activity for this period, the VPN Concentrator Manager session terminates. Minimum is 1, default is 600, and maximum is 1800 seconds (30 minutes).

The Manager resets the inactivity timer only when you click an action button (**Apply**, **Add**, **Cancel**, etc.) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen *does not* reset the timer.

Session Limit

Enter the maximum number of simultaneous administrative sessions allowed. Minimum is 1, default is 10, and maximum is 50 sessions.

Encrypt Config File

To encrypt sensitive entries in the CONFIG file, check the box (default). The CONFIG file is in ASCII text format (.INI format). Check this box to encrypt entries such as passwords, keys, and user information.

To use clear text for all CONFIG file entries, clear the box. For maximum security, we do *not* recommend this option.

Apply / Cancel

To save your settings in the active configuration, click **Apply**. The Manager returns to the **Administration | Access Rights** screen.

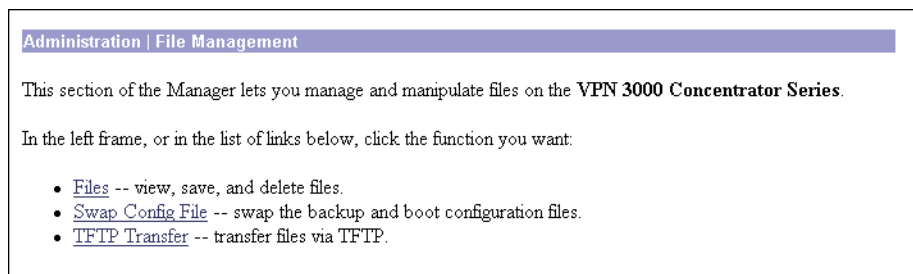
To cancel your settings, click **Cancel**. The Manager returns to the **Administration | Access Rights** screen.

Administration | File Management

This section of the Manager lets you manage files in VPN Concentrator flash memory. (Flash memory acts like a disk.)

- **Files:** copy, view, and delete system files.
- **Swap Configuration Files:** swap backup and boot configuration files.
- **TFTP Transfer:** use TFTP to transfer files to and from the VPN Concentrator.

Figure 14-27: Administration | File Management screen

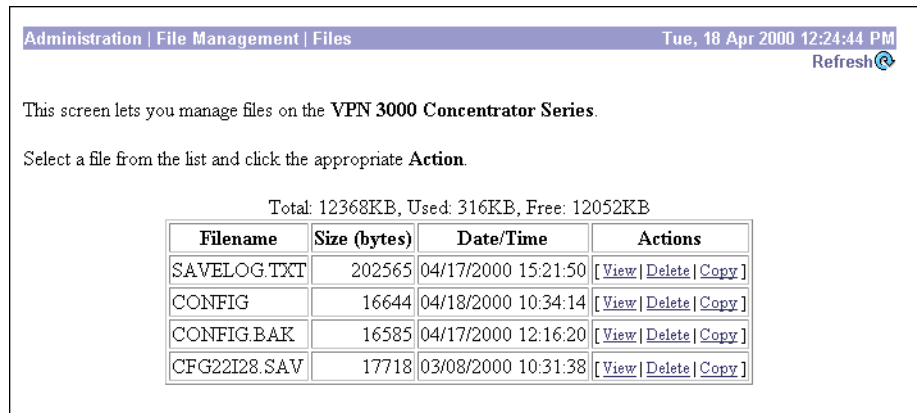



Administration | File Management | Files

This screen lets you manage files in VPN Concentrator flash memory. (Flash memory acts like a disk.) Such files include CONFIG, CONFIG.BAK, LOGNNNNN.TXT files, and copies of them that you have saved under different names.

The screen shows a table listing all files in flash memory, one file per table row. Use the frame scroll controls (if present) to display more files in the table.

Figure 14-28: Administration | File Management | Files screen



Administration | File Management | Files Tue, 18 Apr 2000 12:24:44 PM
Refresh 

This screen lets you manage files on the VPN 3000 Concentrator Series.

Select a file from the list and click the appropriate Action.

Total: 12368KB, Used: 316KB, Free: 12052KB

Filename	Size (bytes)	Date/Time	Actions
SAVELOG.TXT	202565	04/17/2000 15:21:50	[View Delete Copy]
CONFIG	16644	04/18/2000 10:34:14	[View Delete Copy]
CONFIG.BAK	16585	04/17/2000 12:16:20	[View Delete Copy]
CFG22I28.SAV	17718	03/08/2000 10:31:38	[View Delete Copy]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total, Used, Free KB

The total size of flash memory in kilobytes, the amount used by the files listed, and the remaining free space in flash memory.

Filename

The name of the file in flash memory. The VPN Concentrator stores filenames as uppercase in the 8.3 naming convention.

Size (bytes)

The size of the file in bytes.

Date/Time

The date and time the file was created. The format is MM/DD/YY HH:MM:SS, with time in 24-hour notation. For example, 05/07/99 15:20:24 is May 7, 1999 at 3:20:24 PM.

Actions

For a selected file, click the desired action link. The actions available to you depend on your **Access Rights** to **Files**; see the **Administration | Access Rights | Administrators | Modify Properties** screen.

View (Save)

To view the selected file, click **View**. The Manager opens a new browser window to display the file, and the browser address bar shows the filename.

You can also save a copy of the file on the PC that is running the browser. Click the **File** menu on the *new* browser window and select **Save As...** The browser opens a dialog box that lets you save the file. The default filename is the same as on the VPN Concentrator.

Alternatively, you can use the secondary mouse button to click **View** on this Manager screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

Open Link, Open Link in New Window, Open in New Window = Open and view the file in a new browser window, as above.

Save Target As..., Save Link As... = Save a copy of the file on your PC. Your system will prompt for a filename and location. The default filename is the same as on the VPN Concentrator.

When you are finished viewing or saving the file, close the new browser window.

Delete

To delete the selected file from flash memory, click **Delete**. The Manager opens a dialog box for you to confirm or cancel. If you confirm, the Manager refreshes the screen and shows the revised list of files.

Copy

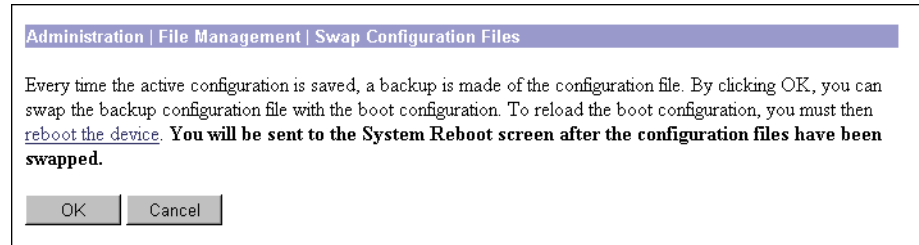
To copy a selected file within flash memory, click **Copy**. The Manager opens a dialog box for you to enter a filename for the copy, and to confirm the action. Filenames must adhere to the 8.3 naming convention. If you confirm, the Manager refreshes the screen and shows the revised list of files.

Administration | File Management | Swap Configuration Files

This screen lets you swap the boot configuration file with the backup configuration file. Every time you save the active configuration, the system writes it to the CONFIG file, which is the boot configuration file; and it saves the previous CONFIG file as CONFIG.BAK, the backup configuration file.

To reload the boot configuration file and make it the active configuration, you must reboot the system. When you click **OK**, the system automatically goes to the **Administration | System Reboot** screen, where you can reboot the system. You can also click the highlighted link to go to that screen.

Figure 14-29: Administration | File Management | Swap Configuration Files screen



OK / Cancel

To swap CONFIG and CONFIG.BAK files, click **OK**. The Manager goes to the **Administration | System Reboot** screen.

To leave the files unchanged, click **Cancel**. The Manager returns to the **Administration | File Management** screen.

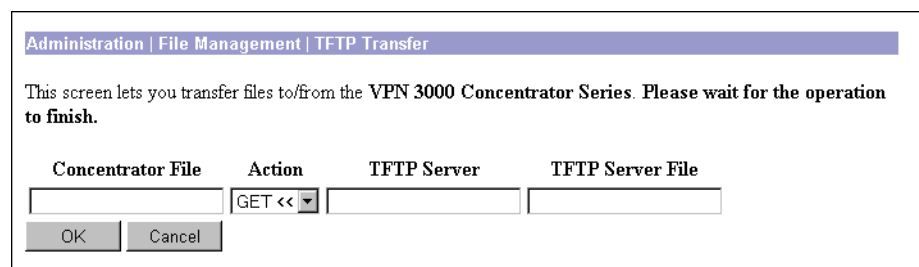
Administration | File Management | TFTP Transfer

This screen lets you use TFTP (Trivial File Transfer Protocol) to transfer files to and from VPN Concentrator flash memory. (Flash memory acts like a disk.) The VPN Concentrator acts as a TFTP client for these functions, accessing a TFTP server running on a remote system. All transfers are made in binary (octet) mode, and they copy—rather than move—files.

To use these functions, you must have **Access Rights** to **Read/Write Files**. See the **Administration | Access Rights | Administrators | Modify Properties** screen.

You can list, view, and manage VPN Concentrator files on the **Administration | File Management | Files** screen.

Figure 14-30: Administration | File Management | TFTP Transfer screen



Concentrator File

Enter the name of the file on the VPN Concentrator. This filename must conform to the 8.3 naming convention.

Action

Click the drop-down menu button and select the TFTP action:

GET << = Get a file from the remote system; i.e., copy a file from the remote system to the VPN Concentrator.

PUT >> = Put a file on the remote system; i.e., copy a file from the VPN Concentrator to the remote system.

TFTP Server

Enter the IP address or hostname of the remote system running the TFTP server. (If you configured a DNS server, you can enter a hostname; otherwise, enter an IP address.)

TFTP Server File

Enter the name of the file on the remote system. This filename must conform to naming conventions applicable to the remote system. *Do not include a path*; the configuration of the remote TFTP server determines the location (path) of the file.

Caution: If either filename is the same as an existing file, TFTP overwrites the existing file without asking for confirmation.

OK / Cancel

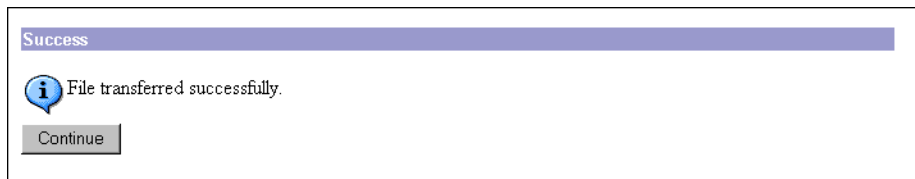
To transfer the file, click **OK**. The Manager pauses during the transfer, which may take a few moments; *please wait for the operation to finish*. The Manager then displays either a **Success** or **Error** screen; see below.

To cancel your settings on this screen, click **Cancel**. The Manager returns to the main **Administration** screen.

Success (TFTP)

If the TFTP transfer is successful, the Manager displays a **Success** screen.

Figure 14-31: Administration | File Management | TFTP Transfer | Success screen



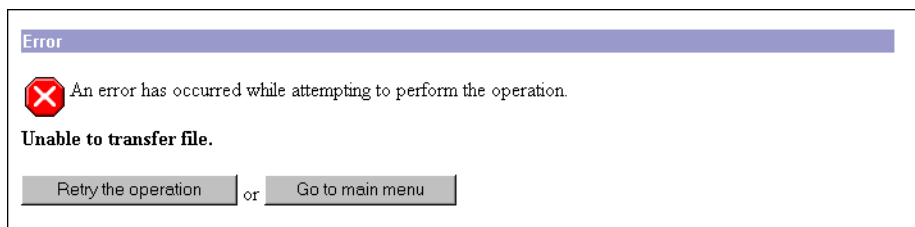
Continue

To return to the **Administration | File Management | TFTP Transfer** screen, click **Continue**.

Error (TFTP)

If the TFTP transfer is unsuccessful for any reason—no such file, incorrect action, remote system unreachable, TFTP server not running, incorrect server address, etc.—the Manager displays an **Error** screen.

Figure 14-32: Administration | File Management | TFTP Transfer | Error screen



To return to the **Administration | File Management | TFTP Transfer** screen, click **Retry the operation**.

To go to the main VPN Concentrator Manager screen, click **Go to main menu**.

Administration | Certificate Management

This section of the Manager lets you manage digital certificates:

- **Enrollment:** create a certificate request to enroll with a Certificate Authority (CA).
- **Installation:** install certificates on the VPN Concentrator.
- **Certificates:** view, delete, configure revocation checking, and generate certificates.

Digital certificates are a form of digital identification used for authentication. CAs issue them in the context of a Public Key Infrastructure (PKI), which uses public-key / private-key encryption to ensure security. CAs are trusted authorities who “sign” certificates to verify their authenticity. The systems on each end of the VPN tunnel must have trusted certificates from the same CA, or from different CAs in a hierarchy of trusted relationships; e.g., “A” trusts “B,” and “B” trusts “C,” therefore “A” trusts “C.”

CAs issue **root** certificates (also known as trusted or signing certificates). They may also issue subordinate trusted certificates. Finally, CAs issue **identity** certificates, which are the certificates for

specific systems or hosts. There must be at least one identity certificate (and its root certificate) on a given VPN Concentrator; there may be more than one root certificate.

During IKE (IPSec) Phase 1 authentication, the communicating parties exchange certificate and key information, and they use the public-key / private-key pairs to generate a hash value; if the hash values match, the client is authenticated.

The VPN Concentrator supports X.509 digital certificates (International Telecommunications Union Recommendation X.509), including SSL (Secure Sockets Layer) certificates that are self-signed or issued in a PKI context.

On the VPN Concentrator, digital certificates are stored as encrypted files in a secure area of flash memory. They do not require you to click **Save Needed** to store them, and they are not visible under **Administration | File Management**.

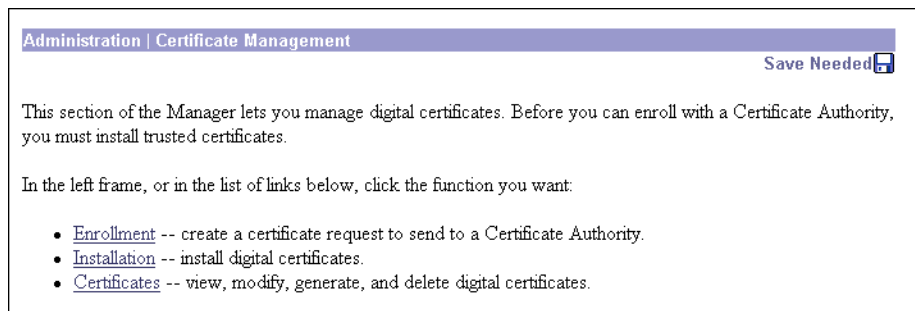
After you install a digital certificate on the VPN Concentrator, it is available in the **Digital Certificate** list for configuring IPSec LAN-to-LAN connections and IPSec SAs. See **Configuration | System | Tunnelling Protocols | IPSec LAN-to-LAN** and **Configuration | Policy Management | Traffic Management | Security Associations**.

The VPN Concentrator can have only one SSL certificate installed. If you generate a self-signed SSL certificate, it replaces any installed PKI-context SSL certificate; and vice-versa.

For information on using SSL certificates, see *Installing the SSL certificate in your browser* in Chapter 1. See also **Configuration | System | Management Protocols | HTTP/HTTPS** and **Telnet**, and **Configuration | System | Management Protocols | SSL**.

Digital certificates carry a timestamp that determines a time frame for their validity. Therefore, it is essential that the time on the VPN Concentrator is correct and synchronized with network time. See **Configuration | System | Servers | NTP** and **Configuration | System | General | Time and Date**.

Figure 14-33: Administration | Certificate Management screen



Installing digital certificates on the VPN Concentrator

Installing a digital certificate on the VPN Concentrator requires these steps:

- 1** Use the **Administration | Certificate Management | Enrollment** screen to generate a certificate request. Save the request as a file, or copy it to the clipboard.
- 2** Send the certificate request to a CA, usually using the CA's Web interface. Most CAs let you submit the request by pasting from the clipboard; otherwise, you can send a file.
- 3** From the CA, receive root (and perhaps subordinate) and identity certificates. *Save them as text files* on your PC or other reachable network host; do not open them or install them in your browser.
- 4** Use the **Administration | Certificate Management | Installation** screen to:
 - a** Install the root certificate on the VPN Concentrator first.
 - b** Then install any subordinate certificate(s).
 - c** Finally, install the identity certificate.
- 5** Use the **Administration | Certificate Management | Certificates** screen to view the certificates and check them, and perhaps to enable revocation checking.
(You must complete the enrollment and certificate installation process within one week of generating the request.)

See the appropriate **Administration | Certificate Management** screen for more details.

Administration | Certificate Management | Enrollment

This screen lets you generate a certificate request to send to a CA (Certificate Authority), to enroll the VPN Concentrator in a PKI.

The entries you make on this screen are governed by PKI standards and practices. The fields conform to ITU-T Recommendation X.520: Selected Attribute Types. You must get from the CA *whether to make an entry* and *what to enter* (format, content, and syntax). You must at least enter the **Common Name (CN)**. All entries may appear in your identity certificate.

When you click **Apply**, the system generates a certificate request; see the **Administration | Certificate Management | Enrollment | Request Generated** screen.

Figure 14-34: Administration | Certificate Management | Enrollment screen

Administration | Certificate Management | Enrollment

This section allows you create a certificate request, so that the VPN 3000 Concentrator Series may be enrolled into the PKI. The certificate request may be sent to a CA, which in turn, will send back a certificate. This section may also be used to generate a request for an SSL certificate. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Type in the name of the certificate file below.

Common Name (CN) <input style="width: 60%;" type="text"/>	Enter the common name for the VPN 3000 Concentrator Series to be used in this PKI. For SSL, use the domain name or IP address you will use to connect to this VPN 3000 Concentrator Series.
Organizational Unit (OU) <input style="width: 60%;" type="text"/>	Enter the department.
Organization (O) <input style="width: 60%;" type="text"/>	Enter the Organization or company.
Locality (L) <input style="width: 60%;" type="text"/>	Enter the city or town.
State/Province (SP) <input style="width: 60%;" type="text"/>	Enter the State or Province. Do not abbreviate (i.e. enter <i>Massachusetts</i> , not <i>MA</i>).
Country (C) <input style="width: 20%;" type="text"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (Fully Qualified Domain Name) <input style="width: 60%;" type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator Series to be used in this PKI.
Key Size <input style="width: 60%;" type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA/DSA key pair. Only RSA keys can be used for SSL certificates.

Common Name (CN)

Enter the name for this VPN Concentrator that identifies it in the PKI; e.g., Engineering VPN. Spaces are allowed. You must enter a name in this field.

If you are requesting an SSL certificate, enter the IP address or domain name you use to connect to this VPN Concentrator; e.g., 10.10.147.2.

Organizational Unit (OU)

Enter the name for the department or other organizational unit to which this VPN Concentrator belongs; e.g., CPU Design. Spaces are allowed.

Organization (O)

Enter the name for the company or organization to which this VPN Concentrator belongs; e.g., Altiga Networks. Spaces are allowed.

Locality (L)

Enter the city or town where this VPN Concentrator is located; e.g., Franklin. Spaces are allowed.

State/Province (SP)

Enter the state or province where this VPN Concentrator is located; e.g., Massachusetts. Spell out completely, do not abbreviate. Spaces are allowed.

Country (C)

Enter the country where this VPN Concentrator is located; e.g., US. Use two characters, no spaces, and no periods. This two-character code must conform to ISO 3166 country abbreviations.

Subject Alternative Name (Fully Qualified Domain Name)

Enter the fully qualified domain name for this VPN Concentrator that identifies it in this PKI; e.g., vpn3030.altiga.com. This field is optional. The alternative name is an additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.

Key Size

Click the drop-down menu button and select the algorithm for generating the public-key / private-key pair, and the key size. If you are requesting an SSL certificate, you must select an RSA choice.

RSA 512 bits = Generate 512-bit keys using the RSA (Rivest, Shamir, Adelman) algorithm. This key size provides sufficient security and is the default selection. It is the most common, and requires the least processing.

RSA 768 bits = Generate 768-bit keys using the RSA algorithm. This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key.

RSA 1024 bits = Generate 1024-bit keys using the RSA algorithm. This key size provides high security, and it requires approximately 4 to 8 times more processing than the 512-bit key.

DSA 512 bits = Generate 512-bit keys using DSA (Digital Signature Algorithm).

DSA 768 bits = Generate 768-bit keys using the DSA algorithm.

DSA 1024 bits = Generate 1024-bit keys using the DSA algorithm.

Apply / Cancel

To generate the certificate request, click **Apply**. The Manager displays the **Administration | Certificate Management | Enrollment | Request Generated** screen, and then opens a browser window showing the certificate request. See below.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the **Administration | Certificate Management** screen.

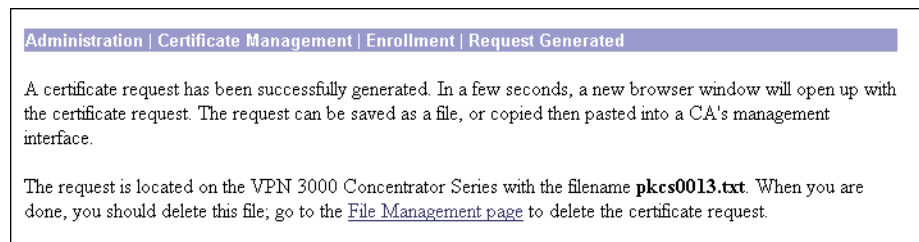
Administration | Certificate Management | Enrollment | Request Generated

The Manager displays this screen when the system has successfully generated a certificate request. The request is a Base-64 encoded file in PKCS-10 format (Public Key Certificate Syntax-10), which most CAs recognize or require. The system automatically saves this file in flash memory with the filename shown in the screen (pkcsNNNN.txt).

In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN Concentrator, and it is not visible.

You must complete the enrollment and certificate installation process within one week of generating the request.

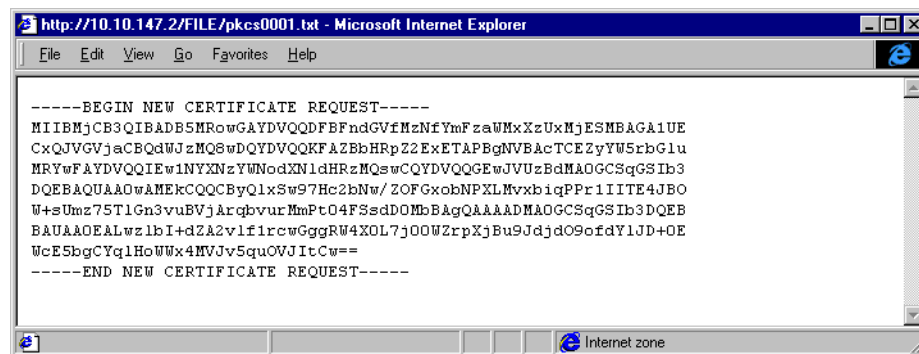
Figure 14-35: Administration | Certificate Management | Enrollment | Request Generated screen



To go to the **Administration | File Management | Files** screen, click the highlighted *File Management page* link. From there you can view, copy, or delete the file in flash memory.

The system also automatically opens a new browser window and displays the certificate request. You can select and copy the request to the clipboard, or you can save it as a file on your PC or a network host. Some CAs let you paste the request on a Web interface, some ask you to send a file; use the method your CA requires.

Figure 14-36: Browser window with PKCS-10 certificate request



Close this browser window when you are finished.

Enrolling with a Certificate Authority

To send the certificate request to a CA, enroll, and receive your digital certificates, follow these steps. (These are cut-and-paste steps; your CA may follow different procedures. In any case, you must end up with certificates *saved as text files* on your PC or other reachable network host.)

- 1 Select and copy the certificate request from the browser window to your clipboard.
- 2 Use a browser to connect to the CA's Web site. Navigate to the screen that lets you submit a PKCS-10 request via cut-and-paste.
- 3 Paste the certificate request in the CA screen, and submit the request.
- 4 The CA should respond with a new browser screen that says the certificates were successfully generated. That screen also should include active links that let you "Download the root certificate" and "Download the identity certificate."
- 5 *With the secondary mouse button*, click the *root* certificate download link and select **Save Link As** or **Save Target As**. You want to *save the file as a text file* on your PC or other reachable network host; *do not open it or install it in the browser*. The browser opens a dialog box that lets you navigate to the desired location and enter a filename. Use a name that clearly identifies this as a root certificate, with a `.txt` extension.
- 6 Repeat the previous step for any subordinate certificates, and finally for the *identity* certificate. Name the files so that you can distinguish the certificate types.
- 7 Proceed to the **Administration | Certificate Management | Installation** screen below.

Administration | Certificate Management | Installation

This Manager screen lets you install digital certificates on the VPN Concentrator.

You can install certificates obtained via enrollment with a CA in a PKI (where the private key is generated on—and stays hidden on—the VPN Concentrator, or you can install certificates imported along with the private key from some source (PKCS-12 format). *The latter certificate installation process is not secure, and we strongly recommend not using it unless you are absolutely certain of its integrity.*

Note: You must install the CA root certificate first, then install any other subordinate certificates from the CA. Install the identity certificate last.

You can also install an SSL server identity certificate issued in a PKI context (not a self-signed SSL certificate). If you install such a certificate, it replaces any self-signed SSL certificate. The VPN Concentrator can have only one SSL certificate, regardless of type.

Figure 14-37: Administration | Certificate Management | Installation screen

Administration | Certificate Management | Installation

This section lets you install certificates onto the VPN 3000 Concentrator Series. **Please wait for the operation to finish.**

Type in the name of the certificate file below.

Certificate Type

Certificate Password

Verify

Local File

Certificate Type

Click the drop-down menu button and select the type of digital certificate to install. (Please note that **--Select a Certificate Type--** is an instruction reminder, not a choice.)

Issuing or Root Certificate Authority = Root and subordinate certificates obtained via enrollment with a CA in a PKI. Select this type and install the root certificate first, then install any subordinate certificates.

SSL Server (via Enrollment) = SSL certificate obtained via enrollment in a PKI.

SSL Server (import with Private Key) = SSL certificate imported along with a private key from some source. *Installing this certificate type is not a completely secure process, and we strongly recommend not using it.* If you select this type, complete the **Certificate Password** and **Verify** fields below.

Server Identity (via Enrollment) = Identity certificates obtained via enrollment with a CA in a PKI. Select this type and install the identity certificate last.

Server Identity (import with Private Key) = Identity certificate imported along with a private key from some source. *Installing this certificate type is not a completely secure process, and we strongly recommend not using it.* If you select this type, complete the **Certificate Password** and **Verify** fields below.

Certificate Password

Complete this field only if you select an **import with Private Key** certificate type. Enter the password for the private key.

Verify

Complete this field only if you select an **import with Private Key** certificate type. Re-enter the private key password to verify it.

Local File / Browse

Enter the complete path and filename of the certificate you are installing; e.g., d:\certs\ca_root.txt. Or click **Browse** to navigate to the file on your PC or other reachable network host.

Apply / Cancel

To install the certificate, click **Apply**. The Manager displays the **Administration | Certificate management | Certificates** screen.

If you select the **Server Identity (import with Private Key)** certificate type, the Manager displays a warning message and asks you confirm.

To discard your entries and cancel the operation, click **Cancel**. The Manager returns to the **Administration | Certificate Management** screen.

Administration | Certificate Management | Certificates

This screen shows all the certificates installed in the VPN Concentrator and lets you view, enable revocation checking, and delete certificates. You can also generate a self-signed SSL server certificate.

The Manager displays this screen each time you install a digital certificate.

Figure 14-38: Administration | Certificate Management | Certificates screen

Administration | Certificate Management | Certificates

This section lets you view certificates on the VPN 3000 Concentrator Series.

Certificate Authorities

Subject	Issuer	Expiration	Actions
Basic Root 1 at CyberTrust Developer Program	Basic Root 1 at CyberTrust Developer Program	06/04/2009	[View] [CRL] [Delete]

Identity Certificates

Subject	Issuer	Expiration	Actions
Tech Pubs VPN at Altiga Networks	Basic CA 1 at CyberTrust Developer Program	03/14/2001	[View] [Delete]

SSL Certificate [[Generate](#)]

Subject	Issuer	Expiration	Actions
10.10.147.2 at Altiga Networks	10.10.147.2 at Altiga Networks	03/11/2003	[View] [Delete]

Certificate Authorities

This table shows installed root and subordinate (trusted) certificates issued by Certificate Authorities (CAs).

Identity Certificates

This table shows installed server identity certificates.

SSL Certificate / [Generate]

This table shows the SSL server certificate installed on the VPN Concentrator. The system can have only one SSL server certificate installed: either a self-signed certificate or one issued in a PKI context.

To generate a self-signed SSL server certificate, click **Generate**. The system uses parameters set on the **Configuration | System | Management Protocols | SSL** screen and generates the certificate. The new certificate replaces any existing SSL certificate.

Subject / Issuer

The Common Name (**CN**) or Organizational Unit (**OU**) (if present), plus the Organization (**O**) in the **Subject** and **Issuer** fields of the certificate. The format is CN at O, OU at O, or just O; e.g., Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See **Administration | Certificate Management | Certificates | View**.

Expiration

The expiration date of the certificate. Format is MM/DD/YYYY.

Actions / View / CRL / Delete

To view details of this certificate, click **View**. The Manager opens the **Administration | Certificate Management | Certificates | View** screen; see below.

To enable CRL (Certificate Revocation List) checking for this CA certificate, click **CRL**. The Manager opens the **Administration | Certificate Management | Certificates | CRL** screen; see below.

To delete this certificate from the VPN Concentrator, click **Delete**. The Manager opens the **Administration | Certificate Management | Certificates | Delete** screen; see below.

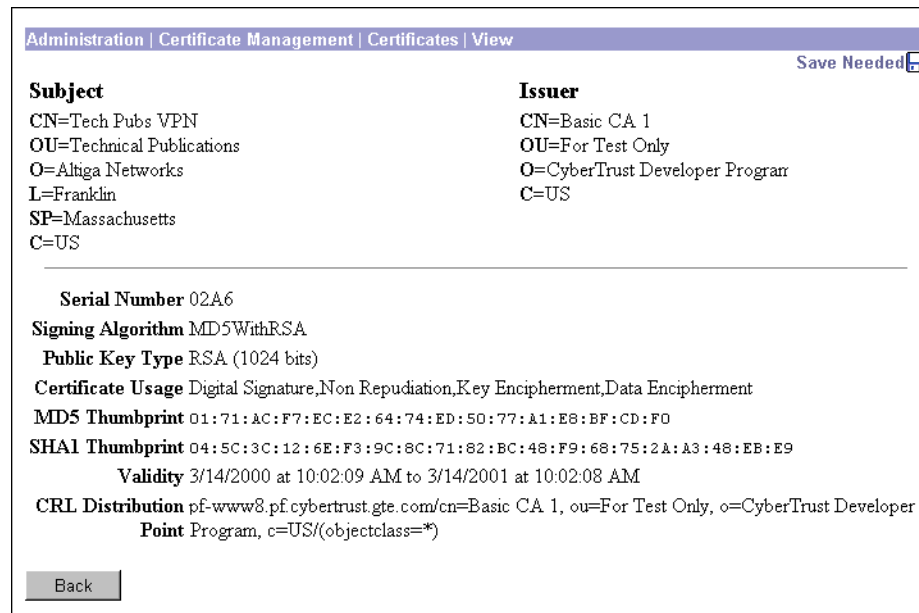
Administration | Certificate Management | Certificates | View

The Manager displays this screen of certificate details when you click **View** for a certificate on the **Administration | Certificate Management | Certificates** screen. The details vary depending on the certificate content.

The content and format for certificate details are governed by ITU (International Telecommunication Union) X.509 standards, specifically RFC 2459. The **Subject** and **Issuer** fields conform to ITU X.520.

This screen is read-only; you cannot change any information here.

Figure 14-39: Administration | Certificate Management | Certificates | View screen



Subject

The person or system that uses the certificate. For a CA root certificate, the **Subject** and **Issuer** are the same.

Issuer

The CA or other entity (jurisdiction) that issued the certificate.

Subject and **Issuer** consist of a specific-to-general identification hierarchy: **CN**, **OU**, **O**, **L**, **SP**, and **C**. These labels and acronyms conform to X.520 terminology, and they echo the fields on the **Administration | Certificate Management | Enrollment** screen.

CN=

Common Name: the name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.

For the VPN Concentrator self-signed SSL certificate, the **CN** is the IP address on the Ethernet 1 (Private) interface at the time the certificate is generated. SSL compares this CN with the address you use to connect to the VPN Concentrator via HTTPS, as part of its validation.

OU=

Organizational Unit: the subgroup within the organization (**O**).

O=

Organization: the name of the company, institution, agency, association, or other entity.

L=

Locality: the city or town where the organization is located.

SP=

State/Province: the state or province where the organization is located.

C=

Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.

Serial Number

The serial number of the certificate. Each certificate issued by a CA or other entity must be unique. CRL checking uses this serial number.

Signing Algorithm

The cryptographic algorithm that the CA or other issuer used to sign this certificate.

Public Key Type

The algorithm and size of the public key that the CA or other issuer used in generating this certificate.

Certificate Usage

The purpose of the key contained in the certificate; e.g., digital signature, certificate signing, nonrepudiation, key or data encipherment, etc.

MD5 Thumbprint

A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.

SHA1 Thumbprint

A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.

Validity

The time period during which this certificate is valid.

Format is MM/DD/YYYY at HH:MM:SS AM/PM to MM/DD/YYYY at HH:MM:SS AM/PM. Time uses 12-hour AM/PM notation, and is local system time.

The Manager checks the validity against the VPN Concentrator system clock, and it flags expired certificates.

Subject Alternative Name (Fully Qualified Domain Name)

The fully qualified domain name for this VPN Concentrator that identifies it in this PKI. The alternative name is an optional additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.

CRL Distribution Point

The distribution point for CRLs (Certificate Revocation Lists) from this CA. If this information is included in the certificate in the proper format, and you enable CRL checking, you do not have to provide it on the **Administration | Certificate Management | Certificates | CRL** screen.

Back

To return to the **Administration | Certificate Management | Certificates** screen, click **Back**.

Administration | Certificate Management | Certificates | CRL

This screen lets you enable Certificate Revocation List (CRL) checking for CA certificates installed in the VPN Concentrator.

A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to a name change, change of association between the subject and the CA, security compromise, etc., the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed Certificate Revocation List (CRL), where each revoked certificate is identified by its

serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the latest CRL to ensure that the certificate has not been revoked.

CAs use LDAP databases to store and distribute CRLs. They may also use other means, but the VPN Concentrator relies on LDAP access.

Since the system has to fetch and examine the CRL from a network distribution point, enabling CRL checking may slow system response times. Also, if the network is slow or congested, CRL checking may fail.

Many certificates include the location of the CRL distribution point. View the certificate to determine its presence. If the CRL distribution point is present in the certificate in the proper format, you need not configure any fields below the checkbox on this screen.

Figure 14-40: Administration | Certificate Management | Certificates | CRL screen

Administration | Certificate Management | Certificates | CRL

Certificate Basic Root 1 at CyberTrust Developer Program

Enable CRL Checking

Server Enter the hostname or IP address of the CRL server.

Server Port Enter the server port number.

Update Period Enter the CRL update period (minutes).

Filter Enter a filter string used to select the CRL (optional).

Base DN Enter the Base DN for the CRL list on the server.

Login DN Enter the Login DN for access to the CRL list on the server.

Password Enter the password for the Login DN.

Verify Verify the password for the Login DN.

Apply Cancel

Certificate

The certificate for which you are configuring CRL checking. This is the name in **Subject** field of **Certificate Authorities** table on **Administration | Certificate Management | Certificates** screen.

Enable CRL Checking

Check this box to enable CRL checking on all certificates issued by this CA under its root. The box is not checked by default.

If this certificate does not include **CRL Distribution Point** information, you must configure the fields that follow. Otherwise, ignore them. Contact the security administrator at the CA to get the proper entries for these fields.

Server

Enter the IP address or hostname of the CRL distribution point server (LDAP server). Maximum 32 characters.

Server Port

Enter the port number for the CRL server. Enter 0 (the default) to have the system supply the default port number, 389 (LDAP).

Update Period

Enter the frequency in minutes to poll for updated CRLs. Enter 0 (the default) to have the system fetch the CRL on demand; i.e., only when the certificate is used for authentication.

Filter

Enter the filename filter (wildcard) to use with the **Base DN** to select the appropriate CRLs in the database. Maximum 128 characters.

Base DN

Enter the LDAP base DN (Distinguished Name), which defines the directory path to the CRL database; e.g., `cn=crl,ou=certs,o=CANam,c=US`. Maximum 128 characters.

Login DN

Enter the login DN to access this CRL database. Maximum 128 characters.

Password

Enter the password for the **Login DN** above. Maximum 128 characters.

Verify

Re-enter the password to verify it. Maximum 128 characters.

Apply / Cancel

To configure CRL checking for this certificate, click **Apply**. The Manager returns to the **Administration | Certificate Management | Certificates** screen.

To discard your settings, click **Cancel**. The Manager returns to the **Administration | Certificate Management | Certificates** screen.

Administration | Certificate Management | Certificates | Delete

The Manager displays this confirmation screen when you click **Delete** for a certificate on the **Administration | Certificate Management | Certificates** screen. The screen shows the same certificate details as on the **Administration | Certificate Management | Certificates | View** screen.

Please note:

- You must delete CA certificates from the bottom up: server identity first, then subordinate CA, then root CA certificates last. Otherwise, the Manager displays an error message.
- If the certificate is in use by an SA, the Manager displays an error message.
- If you delete the SSL certificate, the Manager displays `Error getting SSL Certificate: SSLIOErr` in the **SSL Certificate** table. Generate a new SSL certificate to clear this message.

Figure 14-41: Administration | Certificate Management | Certificates | Delete screen

Administration | Certificate Management | Certificates | Delete Save Needed

Subject	Issuer
CN=100.200.147.2	CN=100.200.147.2
OU=VPN 3000 Concentrator Series	OU=VPN 3000 Concentrator Series
O=Cisco Systems, Inc.	O=Cisco Systems, Inc.
L=Franklin	L=Franklin
SP=Massachusetts	SP=Massachusetts
C=US	C=US

Serial Number 39172897

Signing Algorithm MD5WithRSA

Public Key Type RSA (768 bits)

MD5 Thumbprint C2:28:B6:1C:A6:7D:00:9D:B0:25:E7:06:9B:7E:B0:8B

SHA1 Thumbprint BB:3F:7B:DE:89:38:E6:71:C9:80:DA:8C:11:E8:6E:F5:92:E7:B5:47

Validity 5/8/2000 at 4:50:31 PM to 5/8/2003 at 4:50:31 PM

Are you **sure** you want to delete this certificate?

Yes / No

To delete this certificate, click **Yes**. *There is no undo*. The Manager returns to the **Administration | Certificate Management | Certificates** screen and shows the remaining certificates.

To retain this certificate, click **No**. The Manager returns to the **Administration | Certificate Management | Certificates** screen, and the certificates are unchanged.

End of Chapter



Monitoring

The VPN 3000 Concentrator tracks many statistics and the status of many items essential to system administration and management. This section of the Manager lets you view all those status items and statistics. You can even see the state of LEDs that show the status of hardware subsystems in the device. You can also see statistics that are stored and available in standard MIB-II data objects.

Monitor

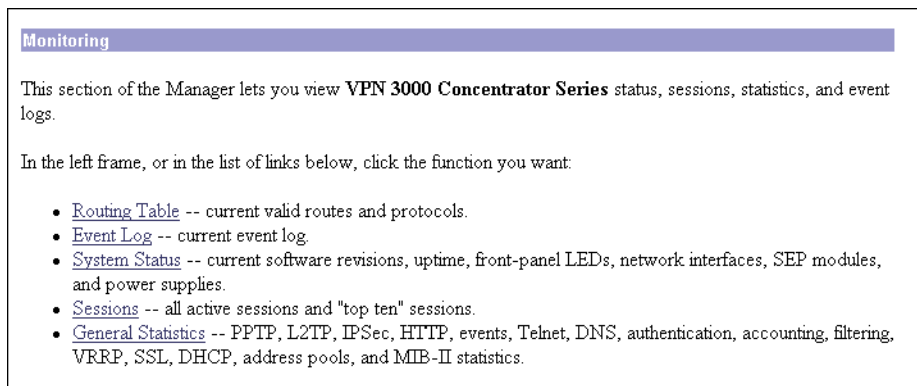
This section of the Manager lets you view VPN Concentrator status, sessions, statistics, and event logs.

- **Routing Table:** current valid routes, protocols, and metrics.
- **Event Log:** current event log in memory.
- **System Status:** current software revisions, uptime, SEP modules, system power supplies, Ethernet interfaces, WAN interfaces, front-panel LEDs, and hardware sensors.
- **Sessions:** currently active sessions sorted by protocol, SEP, and encryption.
 - **Top Ten Lists:** “Top ten” sessions sorted by data, duration, and throughput.
- **General Statistics:** PPTP, L2TP, IPSec, HTTP, events, Telnet, DNS, authentication, accounting, filtering, VRRP, SSL, DHCP, and address pools.
 - **MIB-II Stats:** MIB-II statistics for interfaces, TCP/UDP, IP, RIP, OSPF, ICMP, the ARP table, Ethernet traffic, and SNMP.

These Manager screens are read-only “snapshots” of data or status at the time the screen displays. Most screens have a **Refresh** button that you can click to get a fresh snapshot and update the screen, but you cannot modify the data on the screen.

You can also configure the Manager to automatically refresh all the screens in this section except the **Event Log**. See **Administration | Monitoring Refresh**.

Figure 15-1: Monitor screen



Monitor | Routing Table

This screen shows the VPN Concentrator routing table at the time the screen displays. The IP routing subsystem examines the destination IP address of packets coming through the VPN Concentrator and forwards or drops them according to configured parameters. The routing table shows the valid forwarding paths that the IP routing subsystem knows about, from whatever source: static routes, learned via routing protocols, interface addresses, etc. However, the table lists only the best routes—based on metric and type—with duplicates removed.

To configure routing, see the **Configuration | System | IP Routing** and **Configuration | Interfaces** screens.

Figure 15-2: Monitor | Routing Table screen

The screenshot shows a web interface titled "Monitoring | Routing Table". At the top right, it displays the date and time: "Wed, 03 May 2000 10:28:35 AM" and a "Refresh" button. Below the title, it says "Valid Routes: 177". The main content is a table with the following columns: Address, Mask, Next Hop, Interface, Protocol, Age, and Metric. The table lists 177 routes, with the first 13 visible in the screenshot:

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	100.220.0.57	1	RIP	22	2
100.0.0.0	255.0.0.0	0.0.0.0	1	Local	0	1
212.0.1.0	255.255.255.0	100.49.0.1	1	RIP	8	2
212.0.2.0	255.255.255.0	100.49.0.1	1	RIP	8	2
212.0.3.0	255.255.255.0	100.49.0.1	1	RIP	8	3
212.0.4.0	255.255.255.0	100.49.0.1	1	RIP	8	3
212.0.5.0	255.255.255.0	100.49.0.1	1	RIP	8	4
212.0.6.0	255.255.255.0	100.49.0.1	1	RIP	8	2
212.0.7.0	255.255.255.0	100.49.0.1	1	RIP	8	5
212.0.8.0	255.255.255.0	100.49.0.1	1	RIP	8	2
212.0.9.0	255.255.255.0	100.49.0.1	1	RIP	8	6
212.0.10.0	255.255.255.0	100.49.0.1	1	RIP	8	2
212.0.11.0	255.255.255.0	100.49.0.1	1	RIP	8	4
212.0.12.0	255.255.255.0	100.49.0.1	1	RIP	8	2

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Valid Routes

The total number of current valid routes that the VPN Concentrator knows about. This number includes *all* valid routes, and it may be greater than the number of rows in the routing table, which shows only the best routes with duplicates removed.

Address

The packet destination IP address that this route applies to. This address is combined with the subnet mask to determine the destination route. 0.0.0.0 indicates the default gateway.

Mask

The subnet mask for the destination IP address in the **Address** field. 0.0.0.0 indicates the default gateway.

Next Hop

For remote routes, the IP address of the next system in the path to the destination. 0.0.0.0 indicates a local route; i.e., there is no next hop.

Interface

The VPN Concentrator network interface through which traffic moves on this route:

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.
- 8 or greater = WAN interface.

Protocol

The protocol or source of this routing table entry:

- RIP = learned via Routing Information Protocol.
- OSPF = learned via Open Shortest Path First protocol.
- Static = configured static route.
- Local = local VPN Concentrator interface address.
- ICMP = learned from an ICMP (Internet Control Message Protocol) redirect message.
- Default = the default gateway.

Age

The number of seconds since this route was last updated or otherwise validated. The age is relative to the screen display time; e.g., 25 means the route was last validated 25 seconds before the screen was displayed. 0 indicates a static, local, or default route.

Metric

The metric, or cost, of this route. 1 is lowest, 16 is highest.

Monitor | Event Log

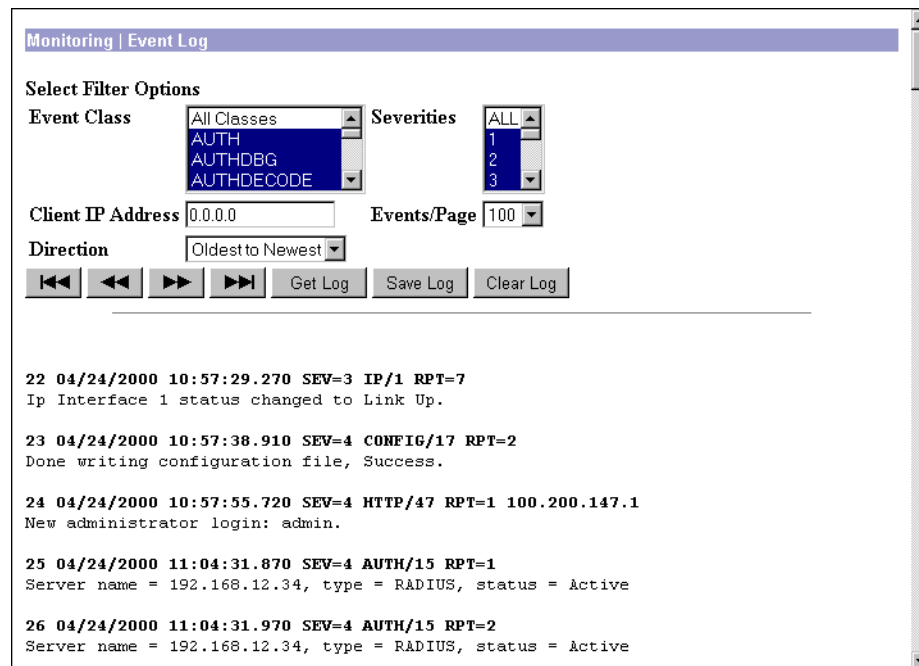
This screen shows the events in the current event log, and lets you manage the event log file. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN Concentrator records events in nonvolatile memory, thus the event log persists even if the system is powered off. The Model 3015–3080 event log holds 2048 events, the Model 3005 holds 256 events, and it wraps when it is full; that is, entry 2049 (or 257) overwrites entry 1, etc. Use the scroll controls (if present) to display more events in the log.

To configure event handling, see the **Configuration | System | Events** screens.

To **Get**, **Save**, or **Clear** the event log file, you must have **Access Rights** to **Read/Write Files**. See the **Administration | Administrators | Modify Properties** screen.

Figure 15-3: Monitor | Event Log screen



Select Filter Options

You can select any or all of the following five options for displaying the event log. After selecting the option(s), click any one of the four **Page** buttons. The Manager refreshes the screen and displays the event log according to your selections.

Your filter options remain in effect as long as you continue working within and viewing **Monitor | Event Log** screens. The Manager resets all options to their defaults if you leave and return, or if you click **Event Log** in the left frame of the Manager window (the table of contents). You cannot save filter options.

Event Class

To display all the events in a single event class, click the drop-down menu button and select the event class. To select a contiguous range of event classes, select the first class in the range, hold down the keyboard **Shift** key, and select the last class in the range. To select multiple event classes, select the first class, hold down the keyboard **Ctrl** key, and select the other classes. By default, the Manager displays **All Classes** of events. Table 10-1 under **Configuration | System | Events** describes the event classes.

Severities

To display all events of a single severity level, click the drop-down menu button and select the severity level. To select a contiguous range of severity levels, select the first severity level in the range, hold down the keyboard **Shift** key, and select the last severity level in the range. To select multiple severity levels, select the first severity level, hold down the keyboard **Ctrl** key, and select the other severity levels. By default, the Manager displays **All** severity levels. See Table 10-2 under **Configuration | System | Events** for an explanation of severity levels.

Client IP Address

To display all events relating to a single IP address, enter the IP address in the field using dotted decimal notation; e.g., 10.10.1.35. By default, the Manager displays all IP addresses. To restore the default, enter 0.0.0.0.

Events/Page

To display a given number of events per Manager screen (page), click the drop-down menu button and select the number. Choices are **10**, **25**, **50**, **100**, **250**, and **ALL**. By default, the Manager displays **100** events per screen.

Direction

To display events in a different chronological order, click the drop-down menu button and select the order. Choices are:

Oldest to Newest = Display events in actual chronological order, with oldest events at the top of the screen. This is the default selection.

Newest to Oldest = Display events in reverse chronological order, with newest events at the top of the screen.

First Page

To display the first page (screen) of the event log, click this button. By default, the Manager displays the first page of the event log when you first open this screen.

Previous Page

To display the previous page (screen) of the event log, click this button.

Next Page

To display the next page (screen) of the event log, click this button.

Last Page

To display the last page (screen) of the event log, click this button.

All four **Page** buttons are also present at the bottom of the screen.

Get Log

To download the event log from VPN Concentrator memory to your PC and view it or save it as a text file, click **Get Log**. The Manager opens a new browser window to display the file. The browser address bar shows the VPN Concentrator address and log file default filename; for example, `http://10.10.4.6/LOG/vpn3000log.txt`.

To save a copy of the log file on your PC, click the **File** menu on the *new* browser window and select **Save As...**. The browser opens a dialog box that lets you save the file. The default filename is `vpn3000log.txt`.

Alternatively, you can use the *secondary* mouse button to click **Get Log** on this **Monitor | Event Log** screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

Open Link, Open Link in New Window, Open in New Window = Open and view the file in a new browser window, as above.

Save Target As..., Save Link As... = Save a copy of the log file on your PC. Your system will prompt for a filename and location. The default filename is `vpn3000log.txt`.

When you are finished viewing or saving the file, close the new browser window.

Save Log

To save a copy of the current event log as a file *on the VPN Concentrator*, click this button. The browser prompts you for a filename, which must conform to the 8.3 naming convention.

Caution: If the filename you enter is the same as an existing file, the browser overwrites the existing file without asking for confirmation.

To list and manage files on the VPN Concentrator, see the **Administration | File Management** screen.

Clear Log

To clear the current event log from memory, click this button. The Manager then refreshes the screen and shows the empty log.

Caution: The Manager immediately erases the event log from memory without asking for confirmation. *There is no undo.*

Event log format

Each entry (record) in the event log consists of eight or nine fields:

```
Sequence Date Time Severity Class/Number Repeat (IPAddress)
String
```

(The `IPAddress` field appears in only certain events.)

For example:

```
3 12/06/1999 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35
New administrator login: admin.
```

Event sequence

The sequential number of the logged entry. Numbering starts or restarts from 1 when the system powers up, when you save the event log, or when you clear the event log. When the log file wraps after 2048 entries (Model 3015–3080; 256 entries on Model 3005), numbering continues with event 2049 (or 257) overwriting event 1. The maximum sequence number is 65536.

Although numbering restarts at 1 when the system powers up, it does *not* overwrite existing entries in the event log; it appends them. Assuming the log doesn't wrap, it could contain several sequences of events starting at 1. Thus you can examine events preceding and following reboot or reset cycles.

Event date

The date of the event: `MM/DD/YYYY`. For example, `12/06/1999` identifies an event that occurred on December 6, 1999.

Event time

The time of the event: `hour:minute:second.millisecond`. The hour is based on a 24-hour clock. For example, `14:37:06.680` identifies an event that occurred at 2:37:06.680 PM.

Event severity

The severity level of the event; for example: `SEV=4` identifies an event of severity level 4. See Table 10-2 under **Configuration | System | Events** for an explanation of severity levels.

Event class / number

The class—or source—of the event, and the internal reference number associated with the specific event within the event class. For example: HTTP/47 identifies that an administrator logged in to the VPN Concentrator using HTTP to connect to the Manager. Table 10-1 under **Configuration | System | Events** describes the event classes. The internal reference number assists Cisco support personnel if they need to examine a log file.

Event repeat

The number of times that this specific event has occurred since the VPN Concentrator was last booted or reset. For example, RPT=17 indicates that this is the 17th occurrence of this specific event.

Event IP address

The IP address of the client or host associated with this event. Only certain events have this field. For tunnel-related events, this is typically the “outer” or tunnel endpoint address. In the **Event log format** example above, 10.10.1.35 is the IP address of the host PC from which admin logged in using the Manager.

Event string

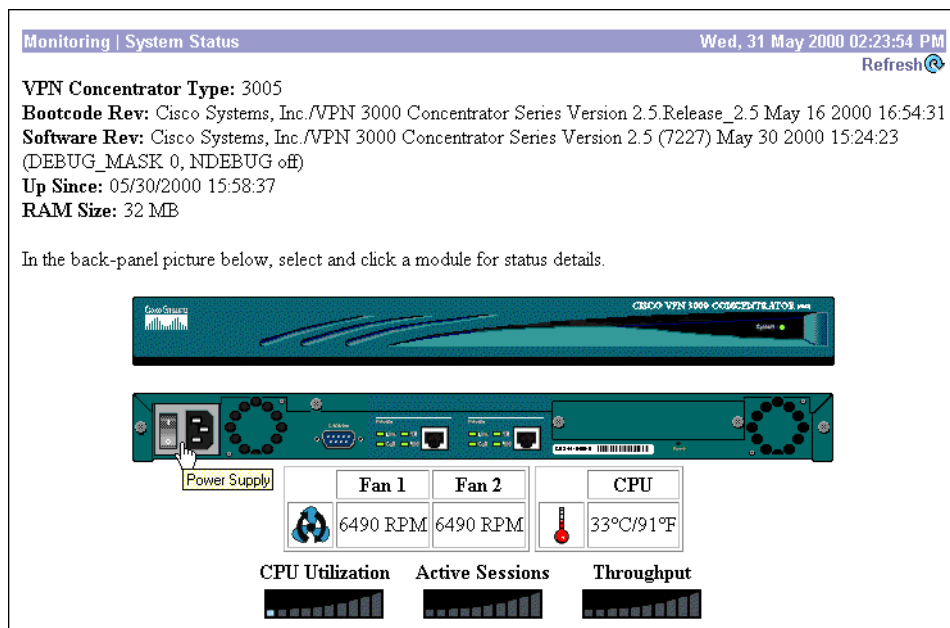
The string, or message, that describes the specific event. Each event class comprises many possible events, and the string gives a brief description. Event strings usually do not exceed 80 characters. In the **Event log format** example above, “New administrator login: admin” describes the event.

Monitor | System Status

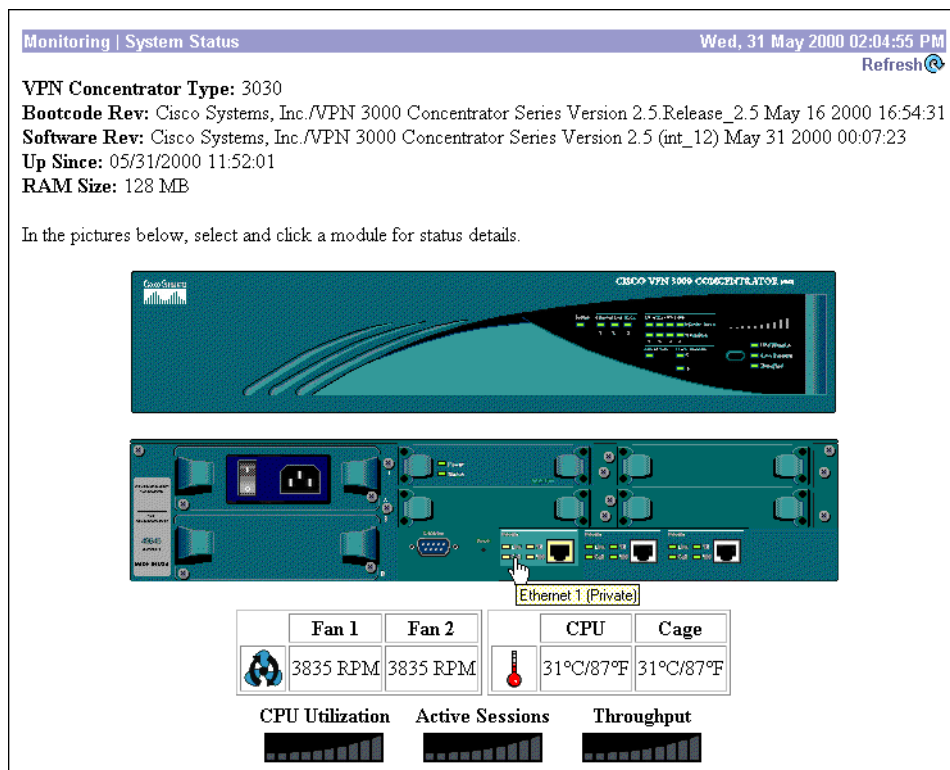
This screen shows the status of several software and hardware variables at the time the screen displays. From this screen you can also display the status and statistics for SEP modules, system power supplies, and network interfaces.

Figure 15-4: Monitor | System Status screen

Model 3005



Model 3015–3080



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

VPN Concentrator Type

The type, or model number, of this VPN Concentrator.

Bootcode Rev

The version name, number, and date of the VPN Concentrator bootcode software file. When you boot or reset the system, the bootcode software runs system diagnostics, and it loads and executes the system software image. The bootcode is installed at the factory, and there is no need to upgrade it. If an engineering change requires a bootcode upgrade, only Cisco support personnel can do so.

Software Rev

The version name, number, and date of the VPN Concentrator system software image file. You can update this image file from the **Administration | Software Update** screen.

Up Since

The date and time that the VPN Concentrator was last booted or reset.

RAM Size

The total amount of SDRAM memory installed in the VPN Concentrator.

Front Panel

*Model
3015–3080 only*

The front panel image is an active link. Put the mouse pointer anywhere within the image and click. The Manager displays the **Monitor | System Status | LED Status** screen.

Back Panel

The back panel image includes active links for configurable modules installed in the VPN Concentrator: Ethernet interfaces, WAN interfaces, power supplies, and SEP modules. Use the mouse pointer to select a module on the back-panel image and click anywhere in the highlighted area. The Manager displays the appropriate **Monitor | System Status | Interface, Power, Dual T1/E1 WAN, or SEP** screen.

Fan 1, Fan 2

The VPN Concentrator includes two cooling fans. In the Model 3005, they are on the rear of the chassis, with Fan 1 on the left as you face the rear. In the Model 3015–3080, they are on the right side of the chassis as you face the front, with Fan 1 closest to the front. This table shows the RPM for both fans. The nominal value is 5000 RPM for the Model 3005 and 3800 RPM for the Model 3015–3080, with an acceptable minimum of 3000 RPM for both. Values below this minimum trigger a hardware event.

CPU, Cage

The VPN Concentrator Model 3015–3080 includes two temperature sensors on the main printed circuit board: one near the CPU and one near the power supply cage. The Model 3005 has one sensor near the CPU. This table shows the temperature at the sensor(s). Temperatures between 0° and 50°C (32° and 122°F) are acceptable. Values outside this range trigger a hardware event.

CPU Utilization

This usage graph shows the CPU load as a percentage of the maximum possible load. Each segment represents 10% of the maximum possible load.

Active Sessions

This usage graph shows the number of active sessions as a percentage of the maximum possible sessions. For example, if 5000 sessions is the maximum, each segment represents 500 sessions. The first segment lights with the first session, the second lights with 10% plus one session, etc.

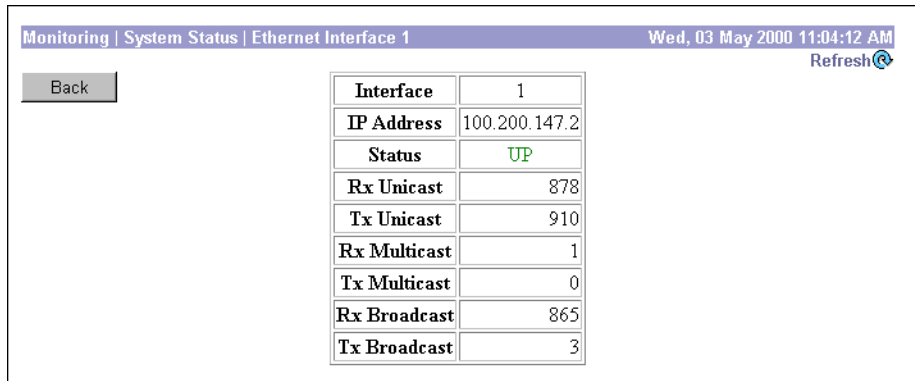
Throughput

This usage graph shows current throughput (measured in LAN packets) as a percentage of the maximum possible system throughput. For example, if two interfaces are set for 100 Mbps, the maximum possible throughput is 200 Mbps and each segment represents 20 Mbps.

Monitor | System Status | Ethernet Interface

This screen displays status and statistics for a VPN Concentrator Ethernet interface. To configure an interface, see **Configuration | Interfaces**.

Figure 15-5: Monitor | System Status | Ethernet Interface screen



Monitoring System Status Ethernet Interface 1		Wed, 03 May 2000 11:04:12 AM
Back		Refresh
Interface	1	
IP Address	100.200.147.2	
Status	UP	
Rx Unicast	878	
Tx Unicast	910	
Rx Multicast	1	
Tx Multicast	0	
Rx Broadcast	865	
Tx Broadcast	3	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the **Monitor | System Status** screen, click **Back**.

Interface

The VPN Concentrator Ethernet interface number:

- 1 = Private interface.
- 2 = Public interface.
- 3 = External interface.

IP Address

The IP address configured on this interface.

Status

The operational status of this interface:

- UP = configured and enabled, ready to pass data traffic.
- DOWN = configured but disabled.

`Testing` = in test mode; no regular data traffic can pass.

`Dormant` = configured and enabled but waiting for an external action, such as an incoming connection.

`Not Present` = missing hardware components.

`Lower Layer Down` = not operational because a lower-layer interface is down.

`Unknown` = not configured.

Rx Unicast

The number of unicast packets that were received by this interface since the VPN Concentrator was last booted or reset. Unicast packets are those addressed to a single host.

Tx Unicast

The number of unicast packets that were routed to this interface for transmission since the VPN Concentrator was last booted or reset, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Rx Multicast

The number of multicast packets that were received by this interface since the VPN Concentrator was last booted or reset. Multicast packets are those addressed to a specific group of hosts.

Tx Multicast

The number of multicast packets that were routed to this interface for transmission since the VPN Concentrator was last booted or reset, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Rx Broadcast

The number of broadcast packets that were received by this interface since the VPN Concentrator was last booted or reset. Broadcast packets are those addressed to all hosts on a network.

Tx Broadcast

The number of broadcast packets that were routed to this interface for transmission since the VPN Concentrator was last booted or reset, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitor | System Status | Dual T1/E1 WAN Slot N

This screen displays status and statistics for a VPN Concentrator WAN module. To configure a WAN module interface, see **Configuration | Interfaces**.

Figure 15-6: Monitor | System Status | Dual T1/E1 WAN Slot N screen

Monitoring System Status Dual T1/E1 WAN Slot 1			Mon, 19 Jun 2000 03:20:18 PM		
Back			Refresh		
T1/E1 Statistics			Synchronous Statistics		
Slot	1	1	Slot	1	1
Port	A	B	Port	A	B
Status	Up	Up	IfIndex	8	9
Up Time Seconds	2205	2207	Status	Up	Up
Errored Seconds	0	0	Protocol	PPP	PPP
Severely Errored Seconds	0	0	Packets Received	2470	1201
Bursty Errored Seconds	0	0	Bytes Received	41242	19296
Severely Errored Framing Seconds	0	0	Packets Transmitted	2348	1275
Unavailable Seconds	564	1240	Bytes Transmitted	38595	20614
Line Errored Seconds	10	6	Received Frame Too Long	0	0
Degraded Minutes	0	0	Transmit Frame Too Long	0	0
Bipolar Violations	603	185	Received Byte Align Errors	61	13
Line Coding Violations	603	185	Received CRC Errors	41	643178
Path Coding Violations	0	0	Receiver Overrun Errors	0	0
Controlled Slips	0	0	Transmits Dropped	0	0
			Transmit Underruns	0	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the **Monitor | System Status** screen, click **Back**.

T1/E1 Statistics

This table shows statistics for the physical T1/E1 interface ports, with a column of statistics for each configured port. RFC 1406 defines most T1/E1 errors.

Slot

The physical slot in the VPN Concentrator (1 through 4) that houses the WAN module.

Port

The interface port on the WAN module (A or B).

Status

The current status of this port:

Up = (Green) Configured, enabled, and operational; synchronized with the network and ready to pass data traffic.

Red = (Red) Red alarm: Port has lost synchronization or signal. This alarm indicates out of frame errors or a mismatched framing format, or a disconnected line.

Blue = (Blue) Blue alarm: A problem on the receive path is causing the port to lose the remote signal. This alarm indicates a problem in the data bit stream.

Yellow = (Yellow) Yellow alarm: A problem on the transmit side (the remote side of the connection has detected a problem with this line).

Loopback = Port is in loopback state.

Unknown = (Red) Not configured or not able to determine status.

Up Time Seconds

The number of seconds this T1/E1 port has been running.

Errored Seconds

The number of seconds during which one or more path coding violations, out-of-frame defects, controlled slips, AIS (Alarm Indication Signal) defects, or bipolar violations was detected on this port. This number excludes unavailable seconds.

Severely Errored Seconds

The number of seconds during which these errors were detected on this port:

- ESF signals: 320 or more path coding violations, one or more out-of-frame defects, or an AIS defect.
- E1/CRC signals: 832 or more path coding violations, or one or more out-of-frame defects.
- E1 signals (no CRC): 2048 or more line coding violations.
- SF/D4 signals: framing errors, one or more out-of-frame defects, or 1544 or more line coding violations.

This number excludes controlled slips and unavailable seconds.

Bursty Errored Seconds

The number of seconds during which one to 319 path coding violations, but no severely errored frame defects or AIS defects, were detected on this port. This number excludes controlled slips and unavailable seconds.

Severely Errored Framing Seconds

The number of seconds during which one or more out-of-frame defects or an AIS defect were detected on this port.

Unavailable Seconds

The number of seconds during which this port has not been available. Basically, unavailable seconds begin with 10 contiguous severely errored seconds, or with a condition leading to failure.

Line Errored Seconds

The number of seconds during which one or more line coding violations were detected on this port.

Degraded Minutes

The number of minutes during which lower than normal-quality signals were detected on this port. (The estimated error rate $>1e^{-6}$ but $<1e^{-3}$.)

Bipolar Violations

The number of bipolar violations detected on this port, defined as:

- AMI-coded signal: a pulse of the same polarity follows the previous pulse.
- B8ZS- or HDB3-coded signal: a pulse of the same polarity follows the previous pulse but is not a part of the zero substitution code.

Line Coding Violations

The number of line coding violations detected on this port, which are bipolar violations or excessive zeros violations (for AMI, >15 contiguous zeros; for B8ZS, >7 contiguous zeros).

Path Coding Violations

The number of path coding violations detected on this port, defined as:

- SF/D4 and E1 (no CRC) signals: a frame synchronization bit error.
- ESF and E1/CRC4 signals: a CRC error.

Controlled Slips

The number of times that the payload bits of a frame were replicated or deleted on this port. This condition occurs when there is a difference between the timing (synchronization) of the receiving port and the received signal.

Synchronous Statistics

This table shows statistics for the synchronous traffic (frames) through the WAN interface ports, with a column of statistics for each configured port.

Slot

The physical slot in the VPN Concentrator (1 through 4) that houses the WAN module.

Port

The interface port on the WAN module (A or B).

IfIndex

The unique interface index (an integer) that identifies this WAN port. For WAN ports, the index integers start at 8.

Status

The current operational status of the port:

`Initializing` = Coming up.

`Running` = Finished initializing; waiting to transition to the `Up` state.

`Up` = (Green) Synchronized and operational; able to transmit and receive packets.

`Down` = (Red) Unable to transmit or receive packets; possibly disconnected from the line.

`Unknown` = (Red) Not configured or unable to determine status.

Protocol

The WAN protocol enabled on this interface:

`MP` = PPP Multilink protocol.

`PPP` = Point-to-Point Protocol.

`Unknown` = Unable to determine protocol.

Packets Received

The number of packets (frames) received on this interface port.

Bytes Received

The number of bytes (octets) received on this interface port.

Packets Transmitted

The number of packets (frames) transmitted on this interface port.

Bytes Transmitted

The number of bytes (octets) transmitted on this interface port.

Received Frame Too Long

The number of received frame too long errors on this interface port. The size of the packets received exceeds the MTU (Maximum Transmission Unit). These errors could indicate that the T1/E1 line is not configured correctly; for example, if you are using a fractional T1/E1 line, the timeslots configured might not match those of the T1/E1 provider.

Transmit Frame Too Long

The number of transmit frame too long errors on this interface port. The size of the transmit packet exceeds the MTU. These errors could indicate that the T1/E1 line is not configured correctly; for example, if you are using a fractional T1/E1 line, the timeslots configured might not match those of the T1/E1 provider.

Received Byte Align Errors

The number of received byte align errors on this interface port. These errors occur when the frame does not contain a multiple of 8 bits, and could indicate misconfigured timeslots.

Received CRC Errors

The number of received CRC (Cyclic Redundancy Checking) errors on this interface port. These errors could indicate a lossy or noisy transmission line.

Receiver Overrun Errors

The number of receiver overrun errors on this interface port. These errors occur when the memory system can't keep up with the incoming data stream. This number should be zero; if not, check the event log for system malfunction or contact technical support.

Transmits Dropped

The number of frames dropped on this interface port because the transmission buffer was full. For example, these errors would occur when trying to transmit too much data from a 100-Mbps Ethernet to a T1/E1 line.

Transmit Underruns

The number of transmission underruns on this interface port. These errors occur when the memory system can't keep up with the outgoing data stream. This number should be zero; if not, check the event log for system malfunction or contact technical support.

Monitor | System Status | Power

This screen displays status and data for VPN Concentrator power supplies and voltage sensors in the system. To configure alarm thresholds for system voltages, see the **Configuration | Interfaces | Power** screen.

Figure 15-7: Monitor | System Status | Power screen

Model 3005

	CPU	Power Supply	Board
2.5V	2.50V		
2.5V Status	OK		
3.3V		3.00V	3.00V
3.3V Status		OK	OK
5V		5.00V	5.00V
5V Status		OK	OK

Model 3015–3080

	CPU	Power Supply A	Power Supply B	Board
2.5V	2.48V			
2.5V Status	OK			
3.3V		2.48V	Not Installed	3.32V
3.3V Status		OK	Not Installed	OK
5V		5.00V	Not Installed	4.97V
5V Status		OK	Not Installed	OK

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the **Monitor | System Status** screen, click **Back**.

CPU

Voltage and status for the voltage sensor on the CPU chip. The screen shows either 1.9 or 2.5 volts, depending on the CPU chip in the system.

Power Supply A, B

Voltages and status for the 3.3- and 5-volt outputs from the power supplies.

Board

Voltages and status for the 3.3- and 5-volt sensors on the main circuit board.

1.9/2.5V Status, 3.3V Status, 5V Status

The status of voltages relative to the configured thresholds:

OK = within low and high threshold limits.

ALARM = outside of low or high threshold limit.

Not Installed = power supply not installed.

Monitor | System Status | SEP

*Model
3015–3080 only*

This screen displays status and statistics for a VPN Concentrator SEP (Scalable Encryption Processing) module, which performs hardware-based cryptographic functions:

- Random-number generation.
- Hash transforms (MD5 and SHA-1) for authentication.
- Encryption and decryption (DES and Triple-DES).

The screen shows cumulative data since the system was last booted or reset.

SEP redundancy

The VPN Concentrator can contain up to four SEP modules for maximum system throughput and redundancy. Two SEP modules provide maximum throughput; additional modules provide redundancy in case of module failure.

SEP redundancy requires no configuration: it is always enabled and completely automatic; no administrator action is required. If a SEP module fails, the VPN Concentrator automatically switches active sessions to another SEP module. If the system has only one SEP module and it fails, the sessions automatically use software cryptographic functions. Even if a SEP module fails, the VPN Concentrator supports the number of sessions for which it is licensed.

If a SEP module fails, the system generates an event of severity level 2. It continues to generate an event every 10 minutes until the failed module is removed or replaced and the VPN Concentrator is rebooted. The front- and back-panel **Status** LEDs also indicate the failed module, as does this screen.

Figure 15-8: Monitor | System Status | SEP screen

SEP		1/CryptSet	
Status	Operational		
DSP Code Version	Dsp Code version 2.1		
	Octets	Packets	
Inbound Hash	4360	0	
Outbound Hash	0	0	
Encrypted	0	0	
Decrypted	3528	0	
Hash Encrypted		0	
Hash Decrypted		52	
Drops		0	
Random Requests		1	
Random Replenishments		1	
Random Bytes Available		1304	
Random Cache Empty		0	
DH Keys Generated		129	
DH Derived Secret Keys		1	
RSA Digital Signings		1	
RSA Digital Verifications		10	
RSA Encryptions	0	0	
RSA Decryptions	34	1	
DSA Digital Keys Generated		0	
DSA Digital Signings		0	
DSA Digital Verifications		0	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the **Monitor | System Status** screen, click **Back**.

SEP

The chassis slot number where this SEP is inserted, and the type of hardware in this SEP:

CryptSet = first-release hardware using a set of integrated circuits.

CryptIC = second-release hardware using a single integrated circuit.

Unknown = hardware could not be determined. *This is an error condition*; please contact Cisco Customer Support.

Status

The functional state of this SEP module:

`Operational` = module is operating correctly.

`Not Operational` = module has failed during operation. *This is an error condition*; please contact Cisco Customer Support.

`Found` = module is installed but is not yet operational. If this condition persists after the VPN Concentrator finishes initializing, it is an error. Please contact Cisco Customer Support.

`Not Found` = module could not be found. *This is an error condition*; please contact Cisco Customer Support.

`Loading` = the system is loading microcode into the SEP module.

`Initializing` = the system is initializing the SEP module.

`Diagnostic Failure` = module failed during diagnostic testing. *This is an error condition*; please contact Cisco Customer Support.

DSP Code Version

The version of DSP (Digital Signal Processing) microcode running on this SEP module. This information may be useful during troubleshooting.

Inbound Hash: Octets / Packets

The number of inbound authentication-only octets (bytes) / packets processed by this SEP. Only hashing algorithms are applied to authentication-only traffic; there is no encryption or decryption.

Outbound Hash: Octets / Packets

The number of outbound authentication-only octets (bytes) / packets processed by this SEP.

Encrypted: Octets / Packets

The number of encryption-only octets (bytes) / packets processed by this SEP. Only encryption algorithms are applied to encryption-only traffic; there is no hashing or authentication.

Decrypted: Octets / Packets

The number of decryption-only octets (bytes) / packets processed by this SEP.

Hash Encrypted: Packets

The number of packets that this SEP processed using both hashing (authentication) and encryption algorithms. This is typical processing for tunneled traffic.

Hash Decrypted: Packets

The number of packets that this SEP processed using both hashing (authentication) and decryption algorithms.

Drops: Packets

The number of packets intended for processing by this SEP, but dropped due to the SEP being overloaded.

Random Requests

The number of requests to this SEP to generate random numbers. When needed (requested), the SEP generates a 2-KB block of random numbers and caches them on the VPN Concentrator. Various cryptographic functions require random numbers of different sizes, and they get them from the cache.

Random Replenishments

The number of times this SEP fulfilled a request to generate a block of random numbers, to replenish the cache.

Random Bytes Available

The number of bytes currently available in the random-number cache on the VPN Concentrator.

Random Cache Empty

The number of times the VPN Concentrator received a request for random numbers and the random-number cache was empty. Since the VPN Concentrator monitors this cache and communicates with the SEP to replenish it, this number should be zero or very small.

DH Keys Generated

The number of times this SEP generated a new Diffie-Hellman key pair. IPSec Security Associations use the Diffie-Hellman algorithm to generate encryption keys, for example.

DH Derived Secret Keys

The number of times this SEP has derived the Diffie-Hellman secret key. In public-key cryptography, the VPN Concentrator receives a remote public key, and the SEP uses the local private key to generate the secret key.

RSA Digital Signings

The number of times this SEP has generated an RSA (Rivest, Shamir, Adelman algorithm) digital signature. The VPN Concentrator generates a digital signature when it creates a digital certificate.

RSA Digital Verifications

The number of times this SEP has verified an RSA digital signature. When the VPN Concentrator receives a signed digital certificate for authentication, it must verify the digital signature by computing a hash of the certificate and comparing it with the received-certificate hash.

RSA Encryptions: Octets / Packets

The number of RSA-encrypted octets (bytes) / packets this SEP has generated.

RSA Decryptions: Octets / Packets

The number of RSA-encrypted octets (bytes) / packets this SEP has received and decrypted.

DSA Digital Keys Generated

The number of times this SEP has generated a new DSA (Digital Signature Algorithm) encryption-key pair.

DSA Digital Signings

The number of times this SEP has generated a DSA digital signature. The VPN Concentrator generates a digital signature when it creates a digital certificate.

DSA Digital Verifications

The number of times this SEP has verified a DSA digital signature. When the VPN Concentrator receives a signed digital certificate for authentication, it must verify the digital signature by computing a hash of the certificate and comparing it with the received-certificate hash.

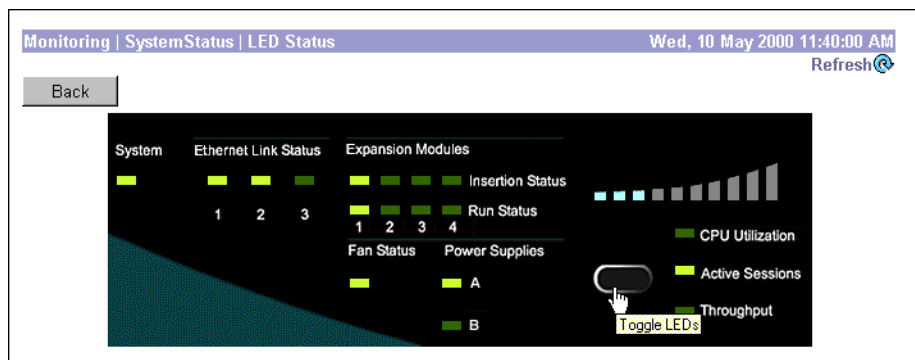
Monitor | System Status | LED Status

*Model
3015–3080 only*

This screen shows the status of VPN Concentrator front-panel LED indicators, exactly as they appear on the unit itself. LED indicators on the VPN Concentrator are normally green, and the usage graph LEDs are blue. LEDs that are amber, red, or off may indicate an error condition. See Appendix A, *Errors and troubleshooting* for descriptions of the LEDs.

The usage graph displays **CPU Utilization**, **Active Sessions**, or **Throughput**, according to the selection you make with the front-panel button. You can “press” the front-panel button either physically—on the unit itself—or logically—on this screen. See **Monitor | System Status** for an explanation of usage graph units.

Figure 15-9: Monitor | System Status | LED Status screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

[LED selector button]

To toggle the usage graph LEDs, click the front-panel button on this screen. Clicking the button here also changes the selection on the VPN Concentrator itself.

Monitor | Sessions

This screen shows comprehensive data for all active user and administrator sessions on the VPN Concentrator.

Figure 15-10: Monitor | Sessions screen

Monitoring | Sessions
Thu, 15 Jun 2000 05:07:18 PM

[Refresh](#)

For more information on a session, click on that session's name.

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	2	3	6	7	1250	33

LAN-to-LAN Sessions

[\[Remote Access Sessions | Management Sessions \]](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
100.to 192	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	Jun 15 15:58:55	1:08:23	7728	17120

Remote Access Sessions

[\[LAN-to-LAN Sessions | Management Sessions \]](#)

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
user1	80.150.0.135	100.177.2.1	PPTP	RC4-128 Stateless	Jun 15 17:05:09	0:02:09	6912	6164
l2tp1	80.150.0.3	100.177.2.2	L2TP	None	Jun 15 17:05:17	0:02:01	6107	9694

Management Sessions

[\[LAN-to-LAN Sessions | Remote Access Sessions \]](#)

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	Local	Console	None	Jun 15 16:59:44	0:07:34
admin	100.200.147.1	HTTP	None	Jun 15 16:55:04	0:12:14
admin	100.150.1.1	HTTP	None	Jun 15 16:31:04	0:36:14

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Session Summary table

This table shows summary totals for LAN-to-LAN, remote access, and management sessions.

A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

Active LAN-to-LAN Sessions

The number of IPSec LAN-to-LAN sessions that are currently active.

Active Remote Access Sessions

The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.

Active Management Sessions

The number of administrator management sessions that are currently active.

Total Active Sessions

The total number of sessions of all types that are currently active.

Peak Concurrent Sessions

The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.

Concurrent Sessions Limit

The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent; e.g., Model 3060 = 5000 sessions.

Total Cumulative Sessions

The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

LAN-to-LAN Sessions table

This table shows parameters and statistics for all active IPSec LAN-to-LAN sessions. Each session here identifies only the outer LAN-to-LAN connection or tunnel, not individual host-to-host sessions within the tunnel.

[Remote Access Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Connection Name

The name of the IPSec LAN-to-LAN connection.

To display detailed parameters and statistics for this connection, click this name. See the **Monitor | Sessions | Detail** screen.

IP Address

The IP address of the remote peer VPN Concentrator or other secure gateway that initiated this LAN-to-LAN connection.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 15-1 on page 15-29 for definitions of these parameters.

Remote Access Sessions table

This table shows parameters and statistics for all active remote-access sessions. Each session is a single-user connection from a remote client to the VPN Concentrator. Remote-access sessions include PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions.

[LAN-to-LAN Sessions | Management Sessions]

Click these active links to go to the other session tables on this Manager screen.

Username

The username or login name for the session. The field shows `Authenticating...` if the remote-access client is still negotiating authentication. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

To display detailed parameters and statistics for this session, click this name. See the **Monitor | Sessions | Detail** screen.

Public IP Address

The public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.

Assigned IP Address

The private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network.

Protocol, Encryption, Login Time, Duration, Bytes Tx, Bytes Rx

See Table 15-1 on page 15-29 for definitions of these parameters.

Management Sessions table

This table shows parameters and statistics for all active administrator management sessions on the VPN Concentrator.

[LAN-to-LAN Sessions | Remote Access Sessions]

Click these active links to go to the other session tables on this Manager screen.

Administrator

The administrator username or login name for the session.

IP Address

The IP address of the manager workstation that is accessing the system. `Local` indicates a direct connection through the **Console** port on the system.

Protocol, Encryption, Login Time, Duration

See Table 15-1 for definitions of these parameters.

Table 15-1: Parameter definitions for Monitor | Sessions screen

Parameter	Definition
Protocol	The protocol this session is using. <code>Console</code> indicates a direct connection through the Console port on the system. See Monitor Sessions Protocols for a graphical representation of sessions by protocol used.
Encryption	The data encryption algorithm this session is using, if any. See Monitor Sessions Encryption for a graphical representation of sessions by encryption algorithm used.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Bytes Tx	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Bytes Rx	The total number of bytes received from the remote peer or client by the VPN Concentrator.

Monitor | Sessions | Detail

These Manager screens show detailed parameters and statistics for a specific remote-access or LAN-to-LAN session. The parameters and statistics differ depending on the session protocol. There are unique screens for:

- IPSec LAN-to-LAN (IPSec/LAN-to-LAN)
- IPSec remote access (IPSec User)
- IPSec through NAT (IPSec/NAT)
- L2TP
- L2TP over IPSec (L2TP/IPSec)
- PPTP

The Manager displays the appropriate screen when you click a highlighted connection name or username on the **Monitor | Sessions** screen. See Figure 15-11 through Figure 15-16 below.

Each session detail screen shows two tables: summary data at the top, and detail data below. The summary data echoes the session data from the **Monitor | Sessions** screen. The session detail table shows all the relevant parameters for each session and subsession.

See Table 15-2 on page 15-34 for definitions of the session detail parameters, in alphabetical order.

Figure 15-11: Monitor | Sessions | Detail screen: IPSec LAN-to-LAN

Monitoring | Sessions | Detail
Thu, 15 Jun 2000 05:08:12 PM

[Refresh](#)

[Back to Sessions](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
100.to 192	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	Jun 15 15:58:56	1:09:16	13664	23056

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		

IPSec Session			
Session ID	2	Remote Address	192.168.84.0/0.0.0.255
Local Address	100.0.0.0/0.255.255.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Bytes Received	23056	Bytes Transmitted	13664

Figure 15-12: Monitor | Sessions | Detail screen: IPSec remote access user


Monitoring Sessions Detail								
							Thu, 15 Jun 2000 05:13:39 PM	
							Refresh 	
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
client	80.150.0.1	100.177.2.4	IPSec	3DES-168	Jun 15 17:11:24	0:02:15	0	0
IKE Sessions: 1								
IPSec Sessions: 1								
IKE Session								
Session ID	1		Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5		Diffie-Hellman Group	Group 1 (768-bit)				
Authentication Mode	Pre-Shared Keys		IKE Negotiation Mode	Aggressive				
IPSec Session								
Session ID	2		Remote Address	100.177.2.4				
Local Address	200.70.50.7		Encryption Algorithm	3DES-168				
Hashing Algorithm	MD5		SEP	1				
Idle Time	0:02:15		Encapsulation Mode	Tunnel				
Bytes Received	0		Bytes Transmitted	0				

Figure 15-13: Monitor | Sessions | Detail screen: IPSec through NAT

Monitoring Sessions Detail								Thu, 15 Jun 2000 05:13:08 PM		
								Refresh		
Back to Sessions										
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
client2	80.177.1.3	100.177.2.3	IPSec/NAT	3DES-168	Jun 15 17:10:53	0:02:15	864	600		
IKE Session										
Session ID		1		Encryption Algorithm		3DES-168				
Hashing Algorithm		MD5		Diffie-Hellman Group		Group 1 (768-bit)				
Authentication Mode		Pre-Shared Keys		IKE Negotiation Mode		Aggressive				
IPSec/NAT Session										
Session ID		2		Remote Address		100.177.2.3				
Local Address		200.70.50.7		Encryption Algorithm		3DES-168				
Hashing Algorithm		MD5		SEP		1				
Idle Time		0:01:09		Encapsulation Mode		Tunnel				
UDP Port		33333								
Bytes Received		120		Bytes Transmitted		120				
IPSec/NAT Session										
Session ID		3		Remote Address		100.177.2.3				
Local Address		100.0.0.0/0.255.255.255		Encryption Algorithm		3DES-168				
Hashing Algorithm		MD5		SEP		1				
Idle Time		0:02:08		Encapsulation Mode		Tunnel				
UDP Port		33333								
Bytes Received		480		Bytes Transmitted		744				

Figure 15-14: Monitor | Sessions | Detail screen: L2TP

Monitoring Sessions Detail								Thu, 15 Jun 2000 05:06:42 PM		
								Refresh		
Back to Sessions										
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx		
l2tp1	80.150.0.3	100.177.2.2	L2TP	None	Jun 15 17:05:17	0:01:25	1967	7390		
L2TP Sessions: 1										
L2TP Session										
Session ID		1		Username		l2tp1				
Assigned IP Address		100.177.2.2		Encryption Algorithm		None				
Authentication Mode		MS-CHAP v1								
Bytes Received		7390		Bytes Transmitted		1967				

Figure 15-15: Monitor | Sessions | Detail screen: L2TP over IPsec



Monitoring Sessions Detail			Thu, 15 Jun 2000 05:14:01 PM					
			Refresh 					
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
dellauser	200.70.50.134	100.177.2.5	L2TP/IPSec	3DES-168	Jun 15 17:12:49	0:01:12	1416	12848
IKE Sessions: 1								
IPSec Sessions: 1								
L2TP Sessions: 1								
IKE Session								
Session ID	1	Encryption Algorithm	3DES-168					
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)					
Authentication Mode	RSA Certificate	IKE Negotiation Mode	Main					
Rekey Time Interval	28800 seconds							
IPSec Session								
Session ID	2	Remote Address	200.70.50.134					
Local Address	200.70.50.7	Encryption Algorithm	3DES-168					
Hashing Algorithm	MD5	SEP	1					
Idle Time	0:00:04	Encapsulation Mode	Transport					
Rekey Time Interval	3600 seconds	Rekey Data Interval	250000 KBytes					
Bytes Received	12848	Bytes Transmitted	1416					
L2TP/IPSec Session								
Session ID	3	Username	dellauser					
Assigned IP Address	100.177.2.5	Encryption Algorithm	None					
Idle Time	0:00:38	Authentication Mode	MS-CHAP v1					
Bytes Received	6807	Bytes Transmitted	12					

Figure 15-16: Monitor | Sessions | Detail screen: PPTP

Monitoring Sessions Detail			Thu, 15 Jun 2000 05:06:06 PM					
			Refresh 					
Back to Sessions								
Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
user1	80.150.0.135	100.177.2.1	PPTP	RC4-128 Stateless	Jun 15 17:05:09	0:00:57	0	1968
PPTP Sessions: 1								
PPTP Session								
Session ID	1	Username	user1					
Assigned IP Address	100.177.2.1	Encryption Algorithm	RC4-128 Stateless					
Idle Time	0:00:22	Authentication Mode	MS-CHAP v1					
Bytes Received	1968	Bytes Transmitted	0					

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back to Sessions

To return to the **Monitor | Sessions** screen, click **Back to Sessions**.

Monitor | Sessions | Detail parameters

Table 15-2: Parameter definitions for Monitor | Sessions | Detail screens

Parameter	Definition
Assigned IP Address	The private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address, and it lets the client appear to be a host on the private network.
Authentication Mode	The protocol or mode used to authenticate this session.
Bytes Rx Bytes Received	The total number of bytes received from the remote peer or client by the VPN Concentrator.
Bytes Tx Bytes Transmitted	The total number of bytes transmitted to the remote peer or client by the VPN Concentrator.
Connection Name	The name of the IPSec LAN-to-LAN connection.
Diffie-Hellman Group	The algorithm and key size used to generate IPSec SA encryption keys.
Duration	The elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
Encapsulation Mode	The mode for applying IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication; i.e., what part of the original IP packet has ESP applied.
Encryption Encryption Algorithm	The data encryption algorithm this session is using, if any.
Hashing Algorithm	The algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Idle Time	The elapsed time (HH:MM:SS) between the last communication activity on this session and the last screen refresh.
IKE Negotiation Mode	The IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions:	The total number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
IP Address	The IP address of the remote peer VPN Concentrator or other secure gateway that initiated the IPSec LAN-to-LAN connection.

Table 15-2: Parameter definitions for Monitor | Sessions | Detail screens (continued)

Parameter	Definition
IPSec Sessions:	The total number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session may have two IPSec sessions: one showing the tunnel endpoints, and one showing the private networks reachable through the tunnel.
L2TP Sessions:	The total number of user sessions through this L2TP or L2TP / IPSec tunnel; usually 1.
Local Address	The IP address (and wildcard mask) of the destination host (or network) for this session.
Login Time	The date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
Perfect Forward Secrecy Group	The Diffie-Hellman algorithm and key size used to generate IPSec SA encryption keys using Perfect Forward Secrecy.
PPTP Sessions:	The total number of user sessions through this PPTP tunnel; usually 1.
Protocol	The tunneling protocol that this session is using.
Public IP Address	The public IP address of the client for this remote-access session. This is also known as the “outer” IP address. It is typically assigned to the client by the ISP, and it lets the client function as a host on the public network.
Rekey Data Interval	The lifetime in kilobytes of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	The lifetime in seconds of the IPSec (IKE) SA encryption keys.
Remote Address	The IP address (and wildcard mask) of the remote peer (or network) that initiated this session.
SEP	The Scalable Encryption Module that is handling cryptographic processing for this session.
Session ID	An identifier for session components (subsessions) on this screen. With IPSec, there is one identifier for each SA.
UDP Port	The UDP port number used in an IPSec through NAT connection.
Username	The username or login name for the session. If the client is using a digital certificate for authentication, the field shows the Subject CN or Subject OU from the certificate.

Monitor | Sessions | Protocols

This screen graphically displays the protocols used by currently active user and administrator sessions on the VPN Concentrator.

Figure 15-17: Monitor | Sessions | Protocols screen

The screenshot shows a web interface with a header bar containing 'Monitoring | Sessions | Protocols' and 'Thu, 15 Jun 2000 04:16:32 PM' with a 'Refresh' button. Below the header, it displays 'Active Sessions: 6' and 'Total Sessions: 7'. A table lists various protocols with their session counts and percentages, accompanied by small blue progress bars.

Protocol	Sessions	Percentage
Other	0	0.0%
PPTP	0	0.0%
L2TP	1	16.6%
IPSec	0	0.0%
HTTP	2	33.3%
FTP	0	0.0%
Telnet	0	0.0%
SNMP	0	0.0%
TFTP	0	0.0%
Console	1	16.6%
Debug/Telnet	0	0.0%
Debug/Console	1	16.6%
L2TP/IPSec	0	0.0%
IPSec/LAN-to-LAN	1	16.6%
IPSec/NAT	0	0.0%

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Protocol

The protocol that the session is using.

Other = protocol other than those listed here.

PPTP = Point-to-Point Tunneling Protocol.

L2TP = Layer 2 Tunneling Protocol.
IPSec = Internet Protocol Security tunneling protocol (remote-access users).
HTTP = Hypertext Transfer Protocol (Web browser).
FTP = File Transfer Protocol.
Telnet = terminal emulation protocol.
SNMP = Simple Network Management Protocol.
TFTP = Trivial File Transfer Protocol.
Console = directly connected console; no protocol.
Debug/Telnet = debugging via Telnet (Cisco use only).
Debug/Console = debugging via console (Cisco use only).
L2TP/IPSec = L2TP over IPSec.
IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.
IPSec/NAT = IPSec through NAT (Network Address Translation).

Sessions

The number of active sessions using this protocol. The sum of this column equals the total number of **Active Sessions** above.

Bar Graph

The percentage of sessions using this protocol relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25%.

Percentage

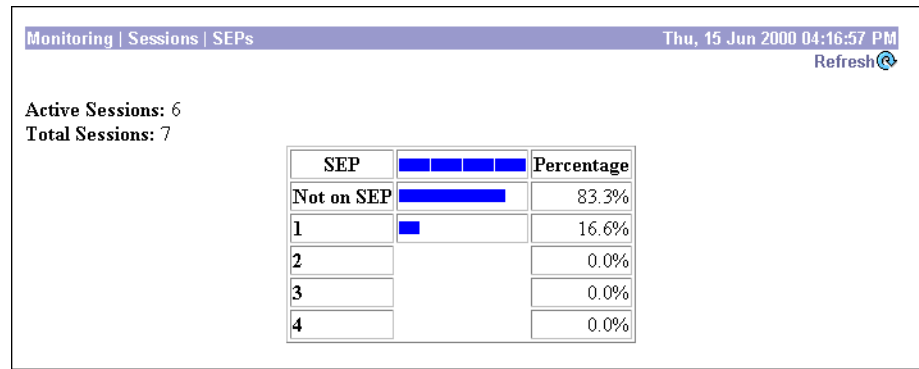
The percentage of sessions using this protocol relative to the total active sessions, as a number. The sum of this column equals 100% (rounded).

Monitor | Sessions | SEPs

*Model
3015–3080 only*

This screen graphically displays the SEP (Scalable Encryption Processing) modules used by currently active user and administrator sessions on the VPN Concentrator. SEP modules perform data encryption functions in hardware.

Figure 15-18: Monitor | Sessions | SEPs screen



Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

SEP

The SEP module that the sessions are using.

Not on SEP = using software encryption, or not using encryption.

1, 2, 3, 4 = SEP module 1, 2, 3, and 4 respectively.

Sessions

The number of active sessions using this SEP module. The sum of this column equals the total number of **Active Sessions** above.

Bar Graph

The percentage of sessions using this SEP module relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25%.

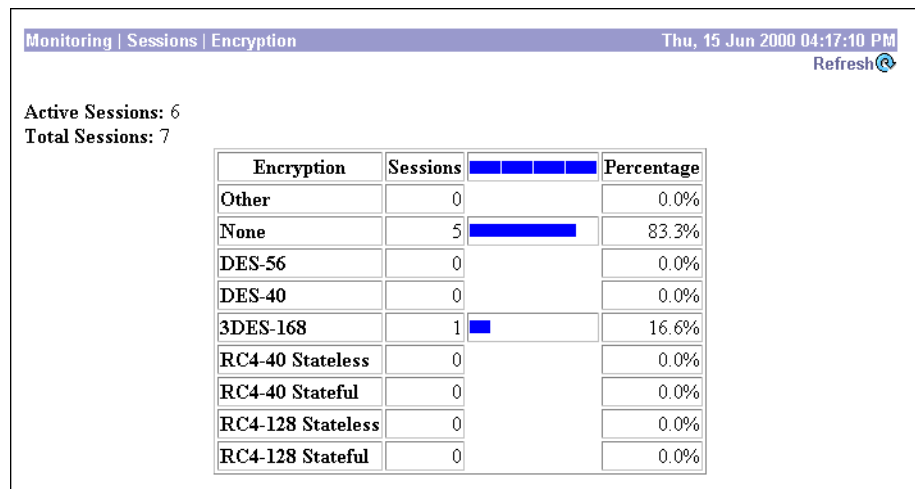
Percentage




The percentage of sessions using this SEP module relative to the total active sessions, as a number. The sum of this column equals 100% (rounded).


Monitor | Sessions | Encryption

This screen graphically displays the data encryption algorithms used by currently active user and administrator sessions on the VPN Concentrator.

Figure 15-19: Monitor | Sessions | Encryption screen



Encryption	Sessions		Percentage
Other	0		0.0%
None	5		83.3%
DES-56	0		0.0%
DES-40	0		0.0%
3DES-168	1		16.6%
RC4-40 Stateless	0		0.0%
RC4-40 Stateful	0		0.0%
RC4-128 Stateless	0		0.0%
RC4-128 Stateful	0		0.0%

Monitoring | Sessions | Encryption Thu, 15 Jun 2000 04:17:10 PM Refresh 

Active Sessions: 6
Total Sessions: 7

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of currently active sessions.

Total Sessions

The total number of sessions since the VPN Concentrator was last booted or reset.

Encryption

The data encryption algorithm that the sessions are using:

Other = other than listed below.

None = no data encryption.

DES-56 = Data Encryption Standard algorithm with a 56-bit key.

DES-40 = DES encryption with a 56-bit key, 40 bits of which are private.

3DES-168 = Triple-DES encryption with a 168-bit key.

RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.

RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.

RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.

RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.

Sessions

The number of active sessions using this encryption algorithm. The sum of this column equals the total number of **Active Sessions** above.

Bar Graph

The percentage of sessions using this encryption algorithm relative to the total active sessions, as a horizontal bar graph. Each segment of the bar in the column heading represents 25%.

Percentage

The percentage of sessions using this encryption algorithm relative to the total active sessions, as a number. The sum of this column equals 100% (rounded).

Monitor | Sessions | Top Ten Lists

This section of the Manager shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by:

- **Data:** total bytes transmitted and received.
- **Duration:** total time connected.
- **Throughput:** average throughput (bytes/sec).

Figure 15-20: Monitor | Sessions | Top Ten Lists screen

Monitoring | Sessions | Top Ten Lists

This section shows statistics for the top 10 currently active sessions, sorted by:

- [Data](#) -- total bytes transmitted and received.
- [Duration](#) -- total time connected.
- [Throughput](#) -- average throughput (bytes/sec).

In the left frame, or in the list of links above, click the sort order you want.

Monitor | Sessions | Top Ten Lists | Data

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by data: total bytes transmitted and received.

Figure 15-21: Monitor | Sessions | Top Ten Lists | Data screen

Monitoring | Sessions | Top Ten Lists | Data Thu, 15 Jun 2000 05:15:31 PM
Refresh

Top Ten users based on **Data** as of 06/15/2000 17:15:21.

Username	IP Address	Protocol	Encryption	Login Time	Total Bytes
200.70.50.5	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	06/15/2000 15:58:55	132840
dellouser	100.177.2.5	L2TP/IPSec	3DES-168	06/15/2000 17:12:49	18576
client2	100.177.2.3	IPSec/NAT	3DES-168	06/15/2000 17:10:53	1704
admin	100.150.1.1	HTTP	None	06/15/2000 16:31:04	N/A
client	100.177.2.4	IPSec	3DES-168	06/15/2000 17:11:23	0
admin	100.200.147.1	HTTP	None	06/15/2000 16:55:04	N/A
admin	Local	Console	None	06/15/2000 16:59:44	N/A

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Username

The login username for the session.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. `Local` identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using.

`Console` = directly connected console; no protocol.

`Debug/Console` = debugging via console (Cisco use only).

`Debug/Telnet` = debugging via Telnet (Cisco use only).

`FTP` = File Transfer Protocol.

`HTTP` = Hypertext Transfer Protocol (Web browser).

`IPSec` = Internet Protocol Security tunneling protocol (remote-access user).

`IPSec/LAN-to-LAN` = IPSec LAN-to-LAN connection.

`IPSec/NAT` = IPSec through NAT (Network Address Translation).

`L2TP` = Layer 2 Tunneling Protocol.

`L2TP/IPSec` = L2TP over IPSec.

`Other` = protocol other than those listed here.

`PPTP` = Point-to-Point Tunneling Protocol.

`SNMP` = Simple Network Management Protocol.

`Telnet` = terminal emulation protocol.

`TFTP` = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using.

`None` = no data encryption.

`DES-40` = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.

`DES-56` = DES encryption with a 56-bit key.

`3DES-168` = Triple-DES encryption with a 168-bit key.

`RC4-40 Stateless` = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.

`RC4-40 Stateful` = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.

`RC4-128 Stateless` = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.

`RC4-128 Stateful` = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Total Bytes

The total number of bytes transmitted and received by this session. N/A = the session is not passing data; e.g., it is an administrator session.

Monitor | Sessions | Top Ten Lists | Duration

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by duration: total time connected.

Figure 15-22: Monitor | Sessions | Top Ten Lists | Duration screen

Username	IP Address	Protocol	Encryption	Login Time	Duration
200.70.50.5	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	06/15/2000 15:58:55	1:16:45
admin	100.150.1.1	HTTP	None	06/15/2000 16:31:04	0:44:36
admin	100.200.147.1	HTTP	None	06/15/2000 16:55:05	0:20:35
admin	Local	Console	None	06/15/2000 16:59:45	0:15:55
client2	100.177.2.3	IPSec/NAT	3DES-168	06/15/2000 17:10:53	0:04:47
client	100.177.2.4	IPSec	3DES-168	06/15/2000 17:11:23	0:04:17
dellouser	100.177.2.5	L2TP/IPSec	3DES-168	06/15/2000 17:12:49	0:02:51

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Username

The login username for the session.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. Local identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using.

`Console` = directly connected console; no protocol.

`Debug/Console` = debugging via console (Cisco use only).

`Debug/Telnet` = debugging via Telnet (Cisco use only).

`FTP` = File Transfer Protocol.

`HTTP` = Hypertext Transfer Protocol (Web browser).

`IPSec` = Internet Protocol Security tunneling protocol (remote-access user).

`IPSec/LAN-to-LAN` = IPSec LAN-to-LAN connection.

`IPSec/NAT` = IPSec through NAT (Network Address Translation).

`L2TP` = Layer 2 Tunneling Protocol.

`L2TP/IPSec` = L2TP over IPSec.

`Other` = protocol other than those listed here.

`PPTP` = Point-to-Point Tunneling Protocol.

`SNMP` = Simple Network Management Protocol.

`Telnet` = terminal emulation protocol.

`TFTP` = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using.

`None` = no data encryption.

`DES-40` = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.

`DES-56` = DES encryption with a 56-bit key.

`3DES-168` = Triple-DES encryption with a 168-bit key.

`RC4-40 Stateless` = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.

`RC4-40 Stateful` = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.

`RC4-128 Stateless` = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.

`RC4-128 Stateful` = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.


Duration

The total amount of time that this session has been connected: HH:MM:SS.

Monitor | Sessions | Top Ten Lists | Throughput

This screen shows statistics for the top 10 currently active VPN Concentrator sessions, sorted by average throughput (bytes/sec).

Figure 15-23: Monitor | Sessions | Top Ten Lists | Throughput screen

Monitoring Sessions Top Ten Lists Throughput						Thu, 15 Jun 2000 05:15:48 PM
						Refresh 
Top Ten users based on Throughput as of 06/15/2000 17:15:21.						
Username	IP Address	Protocol	Encryption	Login Time	Avg. Throughput (bytes/sec)	
delluser	100.177.2.5	L2TP/IPSec	3DES-168	06/15/2000 17:12:49	114	
200.70.50.5	200.70.50.5	IPSec/LAN-to-LAN	3DES-168	06/15/2000 15:58:56	30	
client2	100.177.2.3	IPSec/NAT	3DES-168	06/15/2000 17:10:54	5	
admin	100.150.1.1	HTTP	None	06/15/2000 16:31:04	N/A	
client	100.177.2.4	IPSec	3DES-168	06/15/2000 17:11:24	0	
admin	100.200.147.1	HTTP	None	06/15/2000 16:55:05	N/A	
admin	Local	Console	None	06/15/2000 16:59:45	N/A	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Username

The login username for the session.

IP Address

The IP address of the session user. This is the address assigned to or supplied by a remote user, or the host address of a networked user. `Local` identifies the console directly connected to the VPN Concentrator.

Protocol

The protocol that the session is using.

Console = directly connected console; no protocol.

Debug/Console = debugging via console (Cisco use only).

Debug/Telnet = debugging via Telnet (Cisco use only).

FTP = File Transfer Protocol.

HTTP = Hypertext Transfer Protocol (Web browser).

IPSec = Internet Protocol Security tunneling protocol (remote-access user).

IPSec/LAN-to-LAN = IPSec LAN-to-LAN connection.

IPSec/NAT = IPSec through NAT (Network Address Translation).

L2TP = Layer 2 Tunneling Protocol.

L2TP/IPSec = L2TP over IPSec.

Other = protocol other than those listed here.

PPTP = Point-to-Point Tunneling Protocol.

SNMP = Simple Network Management Protocol.

Telnet = terminal emulation protocol.

TFTP = Trivial File Transfer Protocol.

Encryption

The data encryption algorithm that the session is using.

None = no data encryption.

DES-40 = Data Encryption Standard algorithm with a 56-bit key, 40 bits of which are private.

DES-56 = DES encryption with a 56-bit key.

3DES-168 = Triple-DES encryption with a 168-bit key.

RC4-40 Stateless = RSA RC4 encryption with a 40-bit key, and with keys changed on every packet.

RC4-40 Stateful = RSA RC4 encryption with a 40-bit key, and with keys changed after some number of packets or whenever a packet is lost.

RC4-128 Stateless = RSA RC4 encryption with a 128-bit key, and with keys changed on every packet.

RC4-128 Stateful = RSA RC4 encryption with a 128-bit key, and with keys changed after some number of packets or whenever a packet is lost.

Login Time

The date and time that this session logged in: MM/DD/YYYY HH:MM:SS. Time is in 24-hour notation.

Avg. Throughput (bytes/sec)

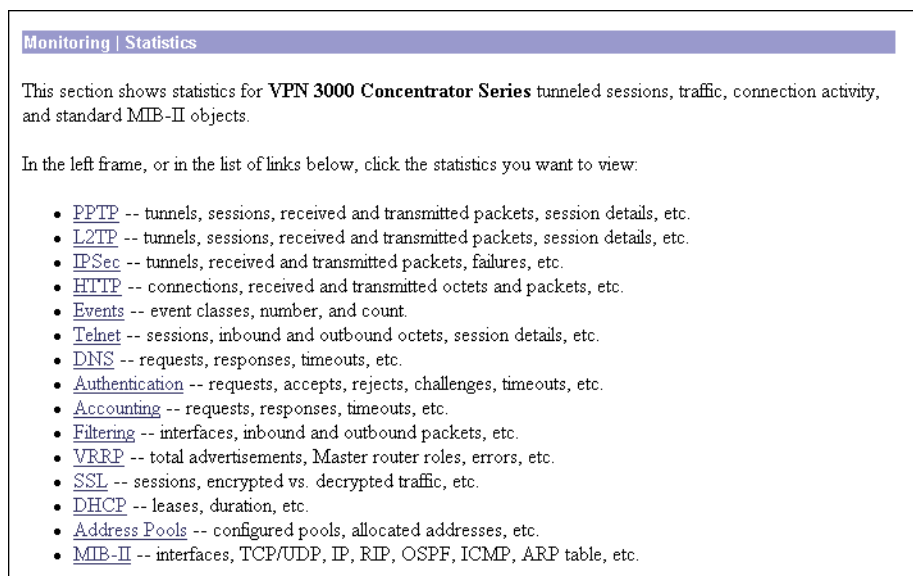
The average throughput of the session, which is [total bytes transmitted and received] divided by total connect time. N/A = the session is not passing data; e.g., it is an administrator session.

Monitor | Statistics

This section of the Manager shows statistics for traffic and activity on the VPN Concentrator since it was last booted or reset, and for current tunneled sessions, plus statistics in standard MIB-II objects for interfaces, TCP/UDP, IP, ICMP, and the ARP table.

- **PPTP**: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- **L2TP**: total tunnels, sessions, received and transmitted control and data packets; and detailed current session data.
- **IPSec**: total Phase 1 and Phase 2 tunnels, received and transmitted packets, failures, drops, etc.
- **HTTP**: total data traffic and connection statistics.
- **Events**: total events sorted by class, number, and count.
- **Telnet**: total sessions, and current session inbound and outbound traffic.
- **DNS**: total requests, responses, timeouts, etc.
- **Authentication**: total requests, accepts, rejects, challenges, timeouts, etc.
- **Accounting**: total requests, responses, timeouts, etc.
- **Filtering**: total inbound and outbound filtered traffic by interface.
- **VRRP**: total advertisements, Master router roles, errors, etc.
- **SSL**: total sessions, encrypted vs. unencrypted traffic, etc.
- **DHCP**: leased addresses, duration, server addresses, etc.
- **Address Pools**: configured pools, allocated and available addresses.
- **MIB-II Stats**: interfaces, TCP/UDP, IP, RIP, OSPF, ICMP, ARP table, Ethernet, and SNMP.

Figure 15-24: Monitor | Statistics screen




Monitor | Statistics | PPTP

This screen shows statistics for PPTP activity on the VPN Concentrator since it was last booted or reset, and for current PPTP sessions.

The **Monitor | Sessions | Detail** screens also show PPTP data.

To configure system-wide PPTP parameters, see the **Configuration | System | Tunneling Protocols | PPTP** screen. To configure PPTP parameters for users and groups, see **Configuration | User Management**. To configure PPTP on rules in filters that govern data traffic, see **Configuration | Policy Management | Traffic Management**.

Figure 15-25: Monitor | Statistics | PPTP screen

Monitoring Statistics PPTP						Thu, 15 Jun 2000 05:08:47 PM		Refresh 		
			Total	Active	Maximum					
	Tunnels		1	1	1					
	Sessions		1	1	1					
		Rx Octets	Rx Packets	Rx Discards	Tx Octets	Tx Packets				
	Control	420	7	0	248	5				
	Data	21845	377	0	12923	201				
PPTP Sessions										
		Receive				Transmit			ACK	
Peer IP	Username	Octets	Packets	Discards	ZLB	Octets	Packets	ZLB	Timeouts	Flow
80.150.0.135	user1	21845	377	0	143	12923	201	37	37	None

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Tunnels

The total number of PPTP tunnels created since the VPN Concentrator was last booted or reset, including those tunnels that failed to be established.

Active Tunnels

The number of PPTP tunnels that are currently active.

Maximum Tunnels

The maximum number of PPTP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Total Sessions

The total number of user sessions through PPTP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The **PPTP Sessions** table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through PPTP tunnels on the VPN Concentrator since it was last booted or reset.

Rx Octets Control / Data

The number of PPTP control / data octets (bytes) received by the VPN Concentrator since it was last booted or reset.

Rx Packets Control / Data

The number of PPTP control / data packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of PPTP control / data packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of PPTP control / data octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of PPTP control / data packets transmitted by the VPN Concentrator since it was last booted or reset.

PPTP Sessions

This table shows statistics for active PPTP sessions on the VPN Concentrator. Each active session is a row.

Peer IP

The IP address of the peer host that established the PPTP tunnel for this session; i.e., the tunnel endpoint IP address. The **Monitor | Sessions** screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within a PPTP tunnel. This is typically the login name of the remote user.

Receive Octets

The total number of PPTP data octets (bytes) received by this session.

Receive Packets

The total number of PPTP data packets received by this session.

Receive Discards

The total number of PPTP data packets received and discarded by this session.

Receive ZLB

The total number of PPTP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of PPTP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of PPTP data packets transmitted by this session.

Transmit ZLB

The total number of PPTP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as GRE acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

ACK Timeouts

The total number of acknowledgement timeouts seen on PPTP data packets for this session. When the system times out waiting for a data packet on which to piggyback an acknowledgement, it sends a ZLB instead. Therefore, this number should equal the **Transmit ZLB** number above.

Flow

The state of packet flow control for this PPTP session:

Local = the local buffer is full; i.e., packet flow for the local end of the session is OFF because the number of outstanding unacknowledged packets received from the peer is equal to the local window size.

Peer = the peer buffer is full; i.e., packet flow for the peer end of the session is OFF because the number of outstanding unacknowledged packets sent to the peer is equal to the peer's window size.

Both = both buffers are full; i.e., packet flow for both ends of the session is OFF because the number of outstanding unacknowledged packets is equal to the window size on both ends.

None = Neither end of the session has a full buffer; i.e., packet flow for the session is ON. This is the normal operating state.


Monitor | Statistics | L2TP

This screen shows statistics for L2TP activity on the VPN Concentrator since it was last booted or reset, and for current L2TP sessions.

The **Monitor | Sessions | Detail** screens also show L2TP data.

To configure system-wide L2TP parameters, see the **Configuration | System | Tunneling Protocols | L2TP** screen. To configure L2TP parameters for users and groups, see **Configuration | User Management**. To configure L2TP on rules in filters that govern data traffic, see **Configuration | Policy Management | Traffic Management**.

Figure 15-26: Monitor | Statistics | L2TP screen

Monitoring Statistics L2TP						Thu, 15 Jun 2000 04:17:41 PM			
Refresh 									
		Total	Active	Maximum	Failed				
Tunnels		1	1	1	0				
Sessions		1	1	1	0				
	Rx Octets	Rx Packets	Rx Discards	Tx Octets	Tx Packets				
Control	501	23	0	452	22				
Data	21959	228	0	769	28				
L2TP Sessions									
			Receive				Transmit		
Remote IP	Username	Serial	Octets	Packets	Discards	ZLB	Octets	Packets	ZLB
80.150.0.3	l2tp1	0	21959	228	0	0	769	28	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Tunnels

The total number of L2TP tunnels successfully established since the VPN Concentrator was last booted or reset.

Active Tunnels

The number of L2TP tunnels that are currently active.

Maximum Tunnels

The maximum number of L2TP tunnels that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Failed Tunnels

The number of L2TP tunnels that failed to become established since the VPN Concentrator was last booted or reset.

Total Sessions

The total number of user sessions successfully established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Active Sessions

The number of user sessions that are currently active through PPTP tunnels. The **L2TP Sessions** table shows statistics for these sessions.

Maximum Sessions

The maximum number of user sessions that have been simultaneously active through L2TP tunnels on the VPN Concentrator since it was last booted or reset.

Failed Sessions

The number of sessions that failed to become established through L2TP tunnels since the VPN Concentrator was last booted or reset.

Rx Octets Control / Data

The number of L2TP control / data channel octets (bytes) received by the VPN Concentrator since it was last booted or reset.

Rx Packets Control / Data

The number of L2TP control / data channel packets received by the VPN Concentrator since it was last booted or reset.

Rx Discards Control / Data

The number of L2TP control / data channel packets received and discarded by the VPN Concentrator since it was last booted or reset.

Tx Octets Control / Data

The number of L2TP control / data channel octets (bytes) transmitted by the VPN Concentrator since it was last booted or reset.

Tx Packets Control / Data

The number of L2TP control / data channel packets transmitted by the VPN Concentrator since it was last booted or reset.

L2TP Sessions

This table shows statistics for active L2TP sessions on the VPN Concentrator. Each active session is a row.

Remote IP

The IP address of the remote host that established the L2TP tunnel for this session; i.e., the tunnel endpoint IP address. The **Monitor | Sessions** screen shows the IP address assigned to the client using the tunnel.

Username

The username for the session within an L2TP tunnel. This is typically the login name of the remote user.

Serial

The serial number of the session within an L2TP tunnel. If there are multiple sessions using a tunnel, each session has a unique serial number.

Receive Octets

The total number L2TP data octets (bytes) received by this session.

Receive Packets

The total number of L2TP data packets received by this session.

Receive Discards

The total number of L2TP data packets received and discarded by this session.

Receive ZLB

The total number of L2TP Zero Length Body acknowledgement data packets received by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Transmit Octets

The total number of L2TP data octets (bytes) transmitted by this session.

Transmit Packets

The total number of L2TP data packets transmitted by this session.

Transmit ZLB

The total number of L2TP Zero Length Body acknowledgement packets transmitted by this session. ZLB packets are sent as acknowledgement packets when there is no data packet on which to piggyback an acknowledgement.

Monitor | Statistics | IPsec

This screen shows statistics for IPsec activity—including current IPsec tunnels—on the VPN Concentrator since it was last booted or reset. These statistics conform to the IETF draft for the IPsec Flow Monitoring MIB.

The **Monitor | Sessions | Detail** screens also show IPsec data.

To configure system-wide IPsec parameters and LAN-to-LAN connections, see the **Configuration | System | Tunneling Protocols | IPsec** screens. To configure IPsec parameters for users and groups, see **Configuration | User Management**. To configure IPsec parameters and SAs on rules in filters that govern data traffic, see **Configuration | Policy Management | Traffic Management**.

Figure 15-27: Monitor | Statistics | IPsec screen

IKE (Phase 1) Statistics		IPsec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	1
Total Tunnels	1	Total Tunnels	1
Received Bytes	2468	Received Bytes	2544
Sent Bytes		Sent Bytes	
Received Packets	30	Received Packets	23
Sent Packets	5	Sent Packets	0
Received Packets Dropped	25	Received Packets Dropped	1
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	0	Sent Packets Dropped	0
Sent Notifies	2	Inbound Authentications	22
Received Phase-2 Exchanges		Failed Inbound Authentications	0
Sent Phase-2 Exchanges		Outbound Authentications	0
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	22
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	0
Phase-2 SA Delete Requests Received	0	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	0	System Capability Failures	
Initiated Tunnels	0	No-SA Failures	
Failed Initiated Tunnels	0	Protocol Use Failures	
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	0		

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IKE (Phase 1) Statistics

This table provides IPsec Phase 1 (IKE: Internet Key Exchange) global statistics. During IPsec Phase 1 (IKE), the two peers establish control tunnels through which they negotiate Security Associations.

Active Tunnels

The number of currently active IKE control tunnels, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IKE control tunnels, both for LAN-to-LAN connections and remote access.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IKE tunnels.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IKE tunnels.

Received Packets

The cumulative total of packets received by all currently and previously active IKE tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IKE tunnels.

Received Packets Dropped

The cumulative total of packets that were dropped during receive processing by all currently and previously active IKE tunnels. If there is a problem with the content of a packet—such as hash failure, parsing error, or encryption failure—received in Phase 1 or the negotiation of Phase 2, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Sent Packets Dropped

The cumulative total of packets that were dropped during send processing by all currently and previously active IKE tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Received Notices

The cumulative total of notify packets received by all currently and previously active IKE tunnels. A notify packet is an informational packet that is sent in response to a bad packet or to indicate status; e.g., error packets, keepalive packets, etc.

Sent Notices

The cumulative total of notify packets sent by all currently and previously active IKE tunnels. See comments for **Received Notices** above.

Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges received by all currently and previously active IKE tunnels; i.e., the total of Phase-2 negotiations received that were initiated by a remote peer. A complete exchange consists of three packets.

Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were sent by all currently and previously active and IKE tunnels; i.e., the total of Phase-2 negotiations initiated by this VPN Concentrator.

Invalid Phase-2 Exchanges Received

The cumulative total of IPSec Phase-2 exchanges that were received, found to be invalid because of protocol errors, and dropped, by all currently and previously active IKE tunnels. In other words, the total of Phase-2 negotiations that were initiated by a remote peer but that this VPN Concentrator dropped because of protocol errors.

Invalid Phase-2 Exchanges Sent

The cumulative total of IPSec Phase-2 exchanges that were sent and were found to be invalid, by all currently and previously active IKE tunnels.

Rejected Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by a remote peer, received, and rejected by all currently and previously active IKE tunnels. Rejected exchanges indicate policy-related failures, such as configuration problems.

Rejected Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by this VPN Concentrator, sent, and rejected, by all currently and previously active IKE tunnels. See comment above.

Phase-2 SA Delete Requests Received

The cumulative total of requests to delete IPSec Phase-2 Security Associations received by all currently and previously active IKE tunnels.

Phase-2 SA Delete Requests Sent

The cumulative total of requests to delete IPsec Phase-2 Security Associations sent by all currently and previously active IKE tunnels.

Initiated Tunnels

The cumulative total of IKE tunnels that this VPN Concentrator initiated. The VPN Concentrator initiates tunnels only for LAN-to-LAN connections.

Failed Initiated Tunnels

The cumulative total of IKE tunnels that this VPN Concentrator initiated and that failed to activate.

Failed Remote Tunnels

The cumulative total of IKE tunnels that remote peers initiated and that failed to activate.

Authentication Failures

The cumulative total of authentication attempts that failed, by all currently and previously active IKE tunnels. Authentication failures indicate problems with preshared keys, digital certificates, or user-level authentication.

Decryption Failures

The cumulative total of decryptions that failed, by all currently and previously active IKE tunnels. This number should be at or near zero; if not, check for misconfiguration or SEP module problems.

Hash Validation Failures

The cumulative total of hash validations that failed, by all currently and previously active IKE tunnels. Hash validation failures usually indicate misconfiguration or mismatched preshared keys or digital certificates.

System Capability Failures

The cumulative total of system capacity failures that occurred during processing of all currently and previously active IKE tunnels. These failures indicate that the system has run out of memory, or that the tunnel count exceeds the system maximum.

No-SA Failures

The cumulative total of nonexistent-Security Association failures that occurred during processing of all currently and previously active IKE tunnels. These failures occur when the system receives a packet for which it has no Security Association, and may indicate synchronization problems.

IPSec (Phase 2) Statistics

This table provides IPSec Phase 2 global statistics. During IPSec Phase 2, the two peers negotiate Security Associations that govern traffic within the tunnel.

Active Tunnels

The number of currently active IPSec Phase-2 tunnels, both for LAN-to-LAN connections and remote access.

Total Tunnels

The cumulative total of all currently and previously active IPSec Phase-2 tunnels, both for LAN-to-LAN connections and remote access.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IPSec Phase-2 tunnels, before decompression. In other words, total bytes of IPSec-only data received by the IPSec subsystem, before decompressing the IPSec payload.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IPSec Phase-2 tunnels, after compression. In other words, total bytes of IPSec-only data sent by the IPSec subsystem, after compressing the IPSec payload.

Received Packets

The cumulative total of packets received by all currently and previously active IPSec Phase-2 tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IPSec Phase-2 tunnels.

Received Packets Dropped

The cumulative total of packets dropped during receive processing by all currently and previously active IPSec Phase-2 tunnels, excluding packets dropped due to anti-replay processing. If there is a problem with the content of a packet, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Received Packets Dropped (Anti-Replay)

The cumulative total of packets dropped during receive processing due to anti-replay errors, by all currently and previously active IPSec Phase-2 tunnels. If the sequence number of a packet is a duplicate or out of bounds, there may be a faulty network or a security breach, and the system drops the packet.

Sent Packets Dropped

The cumulative total of packets dropped during send processing by all currently and previously active IPsec Phase-2 tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Inbound Authentications

The cumulative total number of inbound individual packet authentications performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Inbound Authentications

The cumulative total of inbound packet authentications that failed, by all currently and previously active IPsec Phase-2 tunnels. Failed authentications could indicate corrupted packets or a potential security attack (“man in the middle”).

Outbound Authentications

The cumulative total of outbound individual packet authentications performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Outbound Authentications

The cumulative total of outbound packet authentications that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPsec subsystem problem.

Decryptions

The cumulative total of inbound decryptions performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Decryptions

The cumulative total of inbound decryptions that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check for misconfiguration or SEP module problems.

Encryptions

The cumulative total of outbound encryptions performed by all currently and previously active IPsec Phase-2 tunnels.

Failed Encryptions

The cumulative total of outbound encryptions that failed, by all currently and previously active IPsec Phase-2 tunnels. This number should be zero or very small; if not, check for IPsec subsystem or SEP module problems.

System Capability Failures

The total number of system capacity failures that occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures indicate that the system has run out of memory or some other critical resource; check the event log.

No-SA Failures

The cumulative total of nonexistent-Security Association failures which occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures occur when the system receives an IPsec packet for which it has no Security Association, and may indicate synchronization problems.


Protocol Use Failures

The cumulative total of protocol use failures that occurred during processing of all currently and previously active IPsec Phase-2 tunnels. These failures indicate errors parsing IPsec packets.

Monitor | Statistics | HTTP

This screen shows statistics for HTTP activity on the VPN Concentrator since it was last booted or reset. To configure system-wide HTTP server parameters, see the **Configuration | System | Management | Protocols | HTTP** screen.

Figure 15-28: Monitor | Statistics | HTTP screen

Monitoring Statistics HTTP		Wed, 03 May 2000 01:37:19 PM
		Refresh 
Octets Sent	883727	
Octets Received	508418	
Packets Sent	1801	
Packets Received	1125	
Active Connections	2	
Max Connections	2	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Octets Sent

The total number of HTTP octets (bytes) sent since the VPN Concentrator was last booted or reset.

Octets Received

The total number of HTTP octets (bytes) received since the VPN Concentrator was last booted or reset.

Packets Sent

The total number of HTTP packets sent since the VPN Concentrator was last booted or reset.

Packets Received

The total number of HTTP packets received since the VPN Concentrator was last booted or reset.

Active Connections

The number of currently active HTTP connections.

Max Connections

The maximum number of HTTP connections that have been simultaneously active on the VPN Concentrator since it was last booted or reset.

Monitor | Statistics | Events

This screen shows statistics for all events on the VPN Concentrator since it was last booted or reset.

To configure event handling, see the **Configuration | System | Events** screens.

Figure 15-29: Monitor | Statistics | Events screen

The screenshot shows a web browser window with the title 'Monitoring | Statistics | Events'. The page content includes a table with three columns: 'Event Class', 'Event Number', and 'Count of Events'. The table lists various event classes and their corresponding counts. A 'Refresh' button is visible in the top right corner of the table area.

Event Class	Event Number	Count of Events
PSOS	14	1
PSOS	16	2
PSOS	17	2
PSOS	18	2
PSOS	19	2
PSOS	20	2
PSOS	21	6
PSOS	22	6
PSOS	23	6
QUEUE	1	1
EVENT	37	1
IP	1	3
IP	2	2
HTTP	28	1
HTTP	47	5
AUTH	15	1
PPTP	25	1
CPENC	2	1

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Use the scroll controls (if present) to view the entire table.

Event Class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN Concentrator. Table 10-1 under **Configuration | System | Events** describes the event classes.

Event Number

Event number is an Cisco-assigned reference number that denotes a specific event within the event class. For example, CONFIG event number 2 is “Reading configuration file.” This reference number assists Cisco support personnel if they need to examine event statistics.

Count of Events


The number of times that specific event has occurred on the VPN Concentrator since it was last booted or reset.

Monitor | Statistics | Telnet

This screen shows statistics for Telnet activity on the VPN Concentrator since it was last booted or reset, and for current Telnet sessions.

To configure the VPN Concentrator’s Telnet server, see the **Configuration | System | Management Protocols | Telnet** screen.

Figure 15-30: Monitor | Statistics | Telnet screen

Monitoring Statistics Telnet			Wed, 03 May 2000 01:39:00 PM		
			Refresh 		
Active Sessions		1			
Attempted Sessions		1			
Successful Sessions		1			
Telnet Sessions					
		Inbound Octets		Outbound Octets	
Client IP Address:Port	Total	Command	Discarded	Total	Dropped
100.200.147.1:1324	29	6	0	1218	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of active Telnet sessions. The **Telnet Sessions** table shows statistics for these sessions.

Attempted Sessions

The total number of attempts to establish Telnet sessions on the VPN Concentrator since it was last booted or reset.

Successful Sessions

The total number of Telnet sessions successfully established on the VPN Concentrator since it was last booted or reset.

Telnet Sessions

This table shows statistics for active Telnet sessions on the VPN Concentrator. Each active session is a row.

Client IP Address:Port

The IP address and TCP source port number of this session's remote Telnet client.

Inbound Octets Total

The total number of Telnet octets (bytes) received by this session.

Inbound Octets Command

The number of octets (bytes) containing Telnet commands or options, received by this session.

Inbound Octets Discarded

The number of Telnet octets (bytes) received and dropped during input processing by this session.

Outbound Octets Total

The total number of Telnet octets (bytes) transmitted by this session.

Outbound Octets Dropped

The number of outbound Telnet octets dropped during output processing by this session.

Monitor | Statistics | DNS

This screen shows statistics for DNS (Domain Name System) activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with DNS servers, see the **Configuration | System | Servers | DNS** screen.

Figure 15-31: Monitor | Statistics | DNS screen

The screenshot shows a web interface with a blue header bar containing the text 'Monitoring | Statistics | DNS' on the left and 'Mon, 19 Jun 2000 01:39:17 PM' and a 'Refresh' button on the right. Below the header is a table with the following data:

Requests	18
Responses	18
Timeouts	0
Server Unreachable	0
Other Failures	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests

The total number of DNS queries the VPN Concentrator made since it was last booted or reset. This number equals the sum of the numbers in the four cells below.

Responses

The number of DNS queries that were successfully resolved.

Timeouts

The number of DNS queries that failed because there was no response from the server.

Server Unreachable

The number of DNS queries that failed because the address of the server is not reachable according to the VPN Concentrator's routing table.

Other Failures


The number of DNS queries that failed for an unspecified reason.

Monitor | Statistics | Authentication

This screen shows statistics for user authentication activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with authentication servers, see the **Configuration | System | Servers | Authentication** screens.

Figure 15-32: Monitor | Statistics | Authentication screen

Monitoring Statistics Authentication											Thu, 15 Jun 2000 05:20:23 PM	
Server IP Address:Port	Requests	Retransmissions	Accepts	Rejects	Challenges	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type	Refresh 	
Internal	11	0	11	0	0	0	0	0	0	0		
100.199.7.7:139	0	0	0	0	0	0	0	0	0	0		
100.199.7.7:1645	28	0	28	0	0	0	0	0	0	0		

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address:Port

The IP address of the configured authentication server, and the port number that the VPN Concentrator is using to access the server. Each configured authentication server is a row in this table. `Internal` identifies the internal VPN Concentrator authentication server.

The default, or well-known, port numbers identify an authentication server type:

- 139 = NT Domain
- 389 = LDAP
- 1645 = RADIUS
- 5500 = SDI

Requests

The total number of authentication request packets sent to this server. This number does not include retransmissions.

Retransmissions

The number of authentication request packets retransmitted to this server.

Accepts

The number of authentication acceptance packets received from this server.

Rejects

The number of authentication rejection packets received from this server.

Challenges

The number of authentication challenge packets received from this server.

Malformed Responses

The number of malformed authentication response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of bad authentication response packets received from this server. Bad authenticators contain invalid authenticators or signature attributes.

Pending Requests

The number of authentication request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authentication timeouts to this server. After a timeout the system may retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type

The number of authentication packets of unknown type received from this server.

Monitor | Statistics | Accounting

This screen shows statistics for RADIUS user accounting activity on the VPN Concentrator since it was last booted or reset.

To configure the VPN Concentrator to communicate with RADIUS accounting servers, see the **Configuration | System | Servers | Accounting** screens.

Figure 15-33: Monitor | Statistics | Accounting screen

Monitoring Statistics Accounting								Mon, 19 Jun 2000 02:00:42 PM	
Server IP Address:Port	Requests	Retransmissions	Responses	Malformed Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Type	
100.199.7.7:1646	5	0	5	0	0	0	0	0	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Server IP Address:Port

The IP address of the configured RADIUS user accounting server, and the port number that the VPN Concentrator is using to access the server. Each configured accounting server is a row in this table. The well-known port number for RADIUS accounting is 1646.

Requests

The number of accounting request packets sent to this RADIUS accounting server. This number does not include retransmissions.

Retransmissions

The number of accounting request packets retransmitted to this RADIUS accounting server.

Responses

The number of accounting response packets received from this RADIUS accounting server.

Malformed Responses

The number of malformed accounting response packets received from this RADIUS accounting server. Malformed packets include packets with an invalid length. Bad authenticators are not included in this number.

Bad Authenticators

The number of accounting response packets received from this server that contained invalid authenticators.

Pending Requests

The number of accounting request packets sent to this RADIUS accounting server that have not yet timed out or received a response.

Timeouts

The number of accounting timeouts to this RADIUS server. After a timeout the system may retry the same server, send to a different server, or give up. Retrying the same server is counted as a retransmission as well as a timeout. Sending to a different server is counted as a request as well as a timeout.

Unknown Type


The number of RADIUS packets of unknown type received from this server on the accounting port.

Monitor | Statistics | Filtering

This screen shows statistics for filtering of traffic that has passed through the interfaces on the VPN Concentrator since it was last booted or reset.

To configure filters, see the **Configuration | Policy Management | Traffic Management** screens. To apply filters to interfaces, see the **Configuration | Interfaces** screens. To apply filters to users and groups, see the **Configuration | User Management** screens.

Figure 15-34: Monitor | Statistics | Filtering screen

Monitoring Statistics Filtering							Thu, 15 Jun 2000 04:18:33 PM
							Refresh 
	Inbound Packets			Outbound Packets			
Interface	Pre-Filter	Filtered	Post Filter	Pre-Filter	Filtered	Post Filter	
2	971	138	833	651	0	646	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator network interface through which the filtered traffic has passed.

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.
- 8 or greater = WAN interface.

Inbound Packets Pre-Filter

The total number of inbound packets received on this interface.

Inbound Packets Filtered

The number of inbound packets that have been filtered and dropped on this interface.

Inbound Packets Post Filter

The number of inbound packets that have been filtered and forwarded on this interface. This number equals **Inbound Packets Pre-Filter** minus **Inbound Packets Filtered**.

Outbound Packets Pre-Filter

The total number of outbound packets received on this interface.

Outbound Packets Filtered

The number of outbound packets that have been filtered and dropped on this interface.

Outbound Packets Post Filter


The number of outbound packets that have been filtered and forwarded on this interface. This number equals **Outbound Packets Pre-Filter** minus **Outbound Packets Filtered**.

Monitor | Statistics | VRRP

This screen shows status and statistics for VRRP (Virtual Router Redundancy Protocol) activity on the VPN Concentrator since it was last booted or reset.

To configure VRRP, see the **Configuration | System | IP Routing | Redundancy** screen.

Figure 15-35: Monitor | Statistics | VRRP screen

Monitoring Statistics VRRP		Mon, 19 Jun 2000 01:56:18 PM	
Refresh 			
Checksum Errors	0		
Version Errors	0		
VRID Errors	0		
VRID	1		
Virtual Routers			
	Interface	1 (Private)	2 (Public)
	Status	Master	Master
	Became Master	1	1
	Advertisements Received	0	0
	Advertisement Interval Errors	0	0
	Authentication Failures	0	0
	Time-to-Live Errors	0	0
	Priority 0 Packets Received	0	0
	Priority 0 Packets Sent	0	0
	Invalid Type Received	0	0
	Address List Errors	0	0
	Invalid Authentication Errors	0	0
	Mismatch Authentication Errors	0	0
	Packet Length Errors	0	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Checksum Errors

The total number of VRRP packets received with an invalid VRRP checksum value.

Version Errors

The total number of VRRP packets received with an unknown or unsupported version number. The VPN Concentrator supports VRRP version 2 as defined in RFC 2338.

VRID Errors

The total number of VRRP packets received with an invalid VRRP Group ID number for this VPN Concentrator.

VRID

The identification number that uniquely identifies the group of virtual routers to which this VPN Concentrator belongs.

Not Configured = VRRP has not been configured or enabled.

Virtual Routers

This table shows statistics for the virtual router on each configured VRRP interface on this VPN Concentrator.

Interface: 1 (Private), 2 (Public), 3 (External)

The Ethernet interface configured for VRRP.

Status

The status of the VRRP router in this VPN Concentrator:

Master = VRRP is enabled and the router is functioning as the Master router.

Backup = VRRP is enabled and the router is functioning as a Backup router, monitoring the status of the Master router.

Init = VRRP has been configured but is disabled; i.e., the router is waiting to be enabled (initialized).

Became Master

The total number of times that this VPN Concentrator has become a VRRP Master router after having a different role. This number should be the same in all columns.

Advertisements Received

The total number of VRRP advertisements received by this interface.

Advertisement Interval Errors

The total number of VRRP advertisement packets received by this interface, in which the advertisement interval differs from the interval configured on this VPN Concentrator.

Authentication Failures

The total number of VRRP packets received by this interface that do not pass the authentication check.

Time-to-Live Errors

The total number of VRRP packets received by this interface with IP TTL (Time-To-Live) not equal to 255. All VRRP packets must have TTL = 255.

Priority 0 Packets Received

The total number of VRRP packets received by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Priority 0 Packets Sent

The total number of VRRP packets sent by this interface with a priority of 0. Priority 0 packets indicate that the current Master router has stopped participating in VRRP.

Invalid Type Received

The number of VRRP packets received by this interface with an invalid value in the Type field. For VRRP version 2, the only valid Type value is 1, which indicates an advertisement packet.

Address List Errors

The total number of packets received for which the address list does not match the list configured on this VPN Concentrator.

Invalid Authentication Errors

The total number of packets received by this interface with an unknown authentication type.

Mismatch Authentication Errors

The total number of packets received by this interface with an authentication type that differs from the configured authentication type.

Packet Length Errors

The total number of packets received by this interface with a packet length less than the length of the VRRP header.

Monitor | Statistics | SSL

This screen shows statistics for SSL (Secure Sockets Layer) protocol traffic on the VPN Concentrator since it was last booted or reset.

To configure SSL, see **Configuration | System | Management Protocols | SSL**.

Figure 15-36: Monitor | Statistics | SSL screen

	Inbound Octets	Outbound Octets
Unencrypted	22242	75502
Encrypted	23714	79684
Total Sessions	2	
Active Sessions	2	
Max Active Sessions	2	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Unencrypted Inbound Octets

The number of octets (bytes) of inbound traffic output by the decryption engine.

Encrypted Inbound Octets

The number of octets (bytes) of encrypted inbound traffic sent to the decryption engine. This number includes negotiation traffic.

Unencrypted Outbound Octets

The number of unencrypted outbound octets (bytes) sent to the encryption engine.

Encrypted Outbound Octets

The number of octets (bytes) of outbound traffic output by the encryption engine. This number includes negotiation traffic.

Total Sessions

The total number of SSL sessions.

Active Sessions

The number of currently active SSL sessions.

Max Active Sessions


The maximum number of SSL sessions simultaneously active at any one time.

Monitor | Statistics | DHCP

This screen shows statistics for DHCP (Dynamic Host Configuration Protocol) activity on the VPN Concentrator since it was last booted or reset. Each row of the table shows data for each session using an IP address via DHCP.

To identify DHCP servers to the VPN Concentrator, see **Configuration | System | Servers | DHCP**. To configure system-wide DHCP functions within the VPN Concentrator, see **Configuration | System | IP Routing | DHCP**. To use DHCP to assign addresses to clients, see the **Configuration | System | Address Management | Assignment** screen.

Figure 15-37: Monitor | Statistics | DHCP screen

Monitoring Statistics DHCP					Thu, 15 Jun 2000 05:26:02 PM
					Refresh 
Leased IP Address	Lease Duration	Time Used	Time Left	DHCP Server Address	
100.175.0.2	2:00:00	0:05:21	1:54:39	100.199.7.7	
100.175.0.3	2:00:00	0:05:05	1:54:55	100.199.7.7	
100.175.0.6	2:00:00	0:04:58	1:55:02	100.199.7.7	
100.175.0.7	2:00:00	0:04:46	1:55:14	100.199.7.7	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Leased IP Address

The IP address leased from the DHCP server by the remote client.

Lease Duration

The duration of the current IP address lease, shown as HH:MM:SS.

Time Used

The total length of time that this session has had an active IP address lease, shown as HH:MM:SS.

Time Left

The time remaining until the current IP address lease expires, shown as HH:MM:SS.

DHCP Server Address

The IP address of the DHCP server that leased this IP address.

Monitor | Statistics | Address Pools

This screen shows statistics for address pool activity on the VPN Concentrator since it was last booted or reset. This data appears if the VPN Concentrator is configured to assign IP addresses to clients from an internal address pool.

To configure address pools, see the **Configuration | System | Address Management** screens.

Figure 15-38: Monitor | Statistics | Address Pools screen

The screenshot shows a web interface with a breadcrumb trail 'Monitoring | Statistics | Address Pools' and a timestamp 'Wed, 03 May 2000 02:20:49 PM' with a 'Refresh' button. Below is a table with the following data:

IP Address Range		Addresses			
Start	End	Total	Available	Allocated	Max Allocated
100.200.147.100	100.200.147.177	78	78	0	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IP Address Range: Start / End

The starting and ending IP addresses in the configured address pool. Each configured range is a row in the table.

Total Addresses

The total number of IP addresses in this configured pool.

Available Addresses

The number of IP addresses available (unassigned) in this pool.

Allocated Addresses

The number of IP addresses currently assigned from this pool.

Max Allocated Addresses

The maximum number of IP addresses assigned from this pool at any one time.

Monitor | Statistics | MIB-II

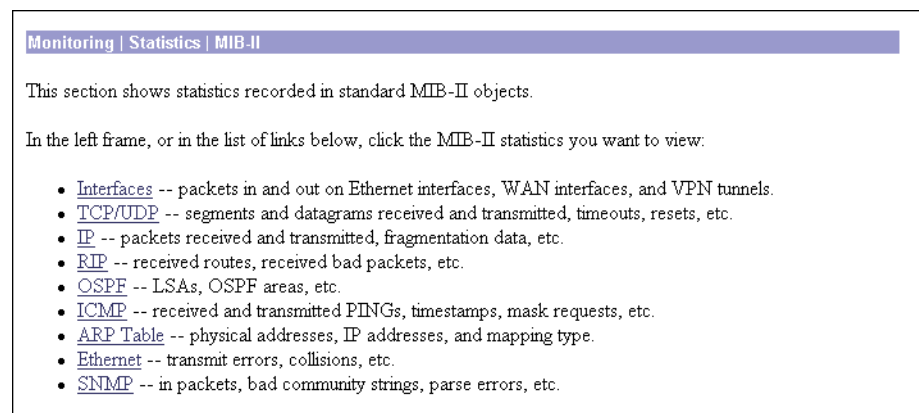
This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN Concentrator. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN Concentrator to gather the data.

Each subsequent screen displays the data for a standard MIB-II group of objects:

- **Interfaces:** packets sent and received on network interfaces and VPN tunnels.
- **TCP/UDP:** Transmission Control Protocol and User Datagram Protocol segments and datagrams sent and received, etc.
- **IP:** Internet Protocol packets sent and received, fragmentation and reassembly data, etc.
- **RIP:** Routing Information Protocol global route changes, bad packets and bad routes received, etc.
- **OSPF:** Open Shortest Path First protocol LSA data, Area data, etc.
- **ICMP:** Internet Control Message Protocol ping, timestamp, and address mask requests and replies, etc.
- **ARP Table:** Address Resolution Protocol physical (MAC) addresses, IP addresses, and mapping types.
- **Ethernet:** errors and collisions, MAC errors, etc.
- **SNMP:** Simple Network Management Protocol requests, bad community strings, parsing errors, etc.

To configure and enable the VPN Concentrator's SNMP server, see the **Configuration | System | Management Protocols | SNMP** screen.

Figure 15-39: Monitor | Statistics | MIB-II screen



Monitor | Statistics | MIB-II | Interfaces

This screen shows statistics in MIB-II objects for VPN Concentrator interfaces since the system was last booted or reset. This screen also shows statistics for VPN tunnels as logical interfaces. RFC 2233 defines interface MIB objects.

Figure 15-40: Monitor | Statistics | MIB-II | Interfaces screen

Monitoring Statistics MIB-II Interfaces		Wed, 03 May 2000 01:40:57 PM					
		Unicast		Multicast		Broadcast	
Interface	Status	In	Out	In	Out	In	Out
Ethernet 1 (Private)	UP	3009	3140	8	0	14017	3
Ethernet 2 (Public)	DOWN	0	0	0	0	0	1

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator interface:

Ethernet 1 (Private) = Ethernet 1 (Private) interface.

Ethernet 2 (Public) = Ethernet 2 (Public) interface.

Ethernet 3 (External) = Ethernet 3 (External) interface.

WAN 1.A = WAN interface module in Slot 1, Port A

WAN 1.B = WAN interface module in Slot 1, Port B

WAN 2.A = WAN interface module in Slot 2, Port A

WAN 2.B = WAN interface module in Slot 2, Port B

1000 and up = VPN tunnels, which are treated as logical interfaces.

Status

The operational status of this interface:

UP = configured and enabled, ready to pass data traffic.

DOWN = configured but disabled.

Testing = in test mode; no regular data traffic can pass.

Dormant = configured and enabled but waiting for an external action, such as an incoming connection.

Not Present = missing hardware components.

Lower Layer Down = not operational because a lower-layer interface is down.

Unknown = not configured.

Unicast In

The number of unicast packets that were received by this interface. Unicast packets are those addressed to a single host.

Unicast Out

The number of unicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Multicast In

The number of multicast packets that were received by this interface. Multicast packets are those addressed to a specific group of hosts.

Multicast Out

The number of multicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Broadcast In

The number of broadcast packets that were received by this interface. Broadcast packets are those addressed to all hosts on a network.

Broadcast Out

The number of broadcast packets that were routed to this interface for transmission, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitor | Statistics | MIB-II | TCP/UDP

This screen shows statistics in MIB-II objects for TCP and UDP traffic on the VPN Concentrator since it was last booted or reset. RFC 2012 defines TCP MIB objects, and RFC 2013 defines UDP MIB objects.

Figure 15-41: Monitor | Statistics | MIB-II | TCP/UDP screen

TCP			UDP	
Segments Received	3023		Datagrams Received	5424
Segments Transmitted	3101		Datagrams Transmitted	0
Segments Retransmitted	1		Errored Datagrams	0
Timeout Min	1000	msec	No Port	2466
Timeout Max	32000	msec		
Connection Limit	-1			
Active Opens	0			
Passive Opens	26			
Attempt Failures	0			
Established Resets	21			
Current Established	2			

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

TCP Segments Received

The total number of segments received, including those received in error and those received on currently established connections. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Transmitted

The total number of segments sent, including those on currently established connections but excluding those containing only retransmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Retransmitted

The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Timeout Min

The minimum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Timeout Max

The maximum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Connection Limit

The limit on the total number of TCP connections that the system can support. A value of -1 means there is no limit.

TCP Active Opens

The number of TCP connections that went directly from an unconnected state to a connection-synchronizing state, bypassing the listening state. These connections are allowed, but they are usually in the minority.

TCP Passive Opens

The number of TCP connections that went from a listening state to a connection-synchronizing state. These connections are usually in the majority.

TCP Attempt Failures

The number of TCP connection attempts that failed. Technically this is the number of TCP connections that went to an unconnected state, plus the number that went to a listening state, from a connection-synchronizing state.

TCP Established Resets

The number of established TCP connections that abruptly closed, bypassing graceful termination.

TCP Current Established

The number of TCP connections that are currently established or are gracefully terminating.

UDP Datagrams Received

The total number of UDP datagrams received. Datagram is the official UDP name for what is casually called a data packet.

UDP Datagrams Transmitted

The total number of UDP datagrams sent. Datagram is the official UDP name for what is casually called a data packet.

UDP Errored Datagrams

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port (**UDP No Port**). Datagram is the official UDP name for what is casually called a data packet.


UDP No Port

The total number of received UDP datagrams that could not be delivered because there was no application at the destination port. Datagram is the official UDP name for what is casually called a data packet.

Monitor | Statistics | MIB-II | IP

This screen shows statistics in MIB-II objects for IP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines IP MIB objects.

Figure 15-42: Monitor | Statistics | MIB-II | IP screen

Monitoring Statistics MIB-II IP		Thu, 15 Jun 2000 04:19:38 PM
Packets Received (Total)	2703	Refresh 
Packets Received (Header Errors)	0	
Packets Received (Address Errors)	0	
Packets Received (Unknown Protocols)	0	
Packets Received (Discarded)	0	
Packets Received (Delivered)	2414	
Packets Forwarded	225	
Outbound Packets Discarded	0	
Outbound Packets with No Route	0	
Packets Transmitted (Requests)	1988	
Fragments Needing Reassembly	0	
Reassembly Successes	0	
Reassembly Failures	0	
Fragmentation Successes	0	
Fragmentation Failures	0	
Fragments Created	0	

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets Received (Total)

The total number of IP data packets received by the VPN Concentrator, including those received with errors.

Packets Received (Header Errors)

The number of IP data packets received and discarded due to errors in IP headers, including bad checksums, version number mismatches, other format errors, etc.

Packets Received (Address Errors)

The number of IP data packets received and discarded because the IP address in the destination field was not a valid address for the VPN Concentrator. This count includes invalid addresses (e.g., 0 . 0 . 0 . 0) and addresses of unsupported classes (e.g., Class E).

Packets Received (Unknown Protocols)

The number of IP data packets received and discarded because of an unknown or unsupported protocol.

Packets Received (Discarded)

The number of IP data packets received that had no problems preventing continued processing, but that were discarded (e.g., for lack of buffer space). This number does not include any packets discarded while awaiting reassembly.

Packets Received (Delivered)

The number of IP data packets received and successfully delivered to IP user protocols (including ICMP) on the VPN Concentrator; i.e., the VPN Concentrator was the final destination.

Packets Forwarded

The number of IP data packets received and forwarded to destinations other than the VPN Concentrator.

Outbound Packets Discarded

The number of outbound IP data packets that had no problems preventing their transmission to a destination, but that were discarded (e.g., for lack of buffer space).

Outbound Packets with No Route

The number of outbound IP data packets discarded because no route could be found to transmit them to their destination. This number includes any packets that the VPN Concentrator could not route because all of its default routers are down.

Packets Transmitted (Requests)

The number of IP data packets that local IP user protocols (including ICMP) supplied to transmission requests. This number does not include any packets counted in **Packets Forwarded**.

Fragments Needing Reassembly

The number of IP fragments received by the VPN Concentrator that needed to be reassembled.

Reassembly Successes

The number of IP data packets successfully reassembled.

Reassembly Failures

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). This number is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

Fragmentation Successes

The number of IP data packets that have been successfully fragmented by the VPN Concentrator.

Fragmentation Failures

The number of IP data packets that have been discarded because they needed to be fragmented but could not be (e.g., because the Don't Fragment flag was set).

Fragments Created

The number of IP data packet fragments that have been generated by the VPN Concentrator.

Monitor | Statistics | MIB-II | RIP

This screen shows statistics in MIB-II objects for RIP version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1724 defines RIP version 2 MIB objects.

To configure RIP on interfaces, see [Configuration | Interfaces](#).

Figure 15-43: Monitor | Statistics | MIB-II | RIP screen

Global Route Changes		176	
Global Queries		0	
Interfaces			
Interface Address	Received Bad Packets	Received Bad Routes	Sent Updates
100.200.147.2	0	0	0
192.168.12.34	0	0	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Global Route Changes

The total number of route changes made to the IP route database by RIP. This number does not include changes that only refresh a route's age.

Global Queries

The total number of responses sent to RIP queries from other systems.

Interfaces

This table shows a row of statistics for each configured interface.

Interface Address

The IP address configured on the interface.

Received Bad Packets

The number of RIP response packets received by this interface that were subsequently discarded for any reason (e.g., wrong version, unknown command type).

Received Bad Routes

The number of routes in valid RIP packets received by this interface that were ignored for any reason (e.g., unknown address family, invalid metric).

Sent Updates


The number of triggered RIP updates actually sent by this interface. This number does not include full updates sent containing new information.

Monitor | Statistics | MIB-II | OSPF

This screen shows statistics in MIB-II objects for OSPF version 2 traffic on the VPN Concentrator since it was last booted or reset. RFC 1850a defines OSPF version 2 MIB objects.

To configure OSPF on interfaces, see **Configuration | Interfaces**. To configure system-wide OSPF parameters, see **Configuration | System | IP Routing**.

Figure 15-44: Monitor | Statistics | MIB-II | OSPF screen

Monitoring Statistics MIB-II OSPF		Thu, 15 Jun 2000 04:20:24 PM			
		Refresh 			
Router ID	200.70.50.7				
Version	2				
External LSA Count	179				
External LSA Checksum	5527500				
LSAs Originated	293				
New LSAs Received	20				
LSA Database Limit	-1				
Designated Routers					
Interface Address	Interface Name	Designated Router	Backup Designated Router		
100.150.7.7	Ethernet 1 (Private)	100.150.7.7	0.0.0.0		
101.197.0.1	Ethernet 3 (External)	0.0.0.0	0.0.0.0		
200.70.50.7	Ethernet 2 (Public)	200.70.50.2	200.70.50.5		
Neighbors					
IP Address	Router ID	State			
200.70.50.2	80.150.5.5	Full			
200.70.50.5	200.70.50.5	Full			
Areas					
Area ID	SPF Runs	AS Border Routers	Area Border Routers	Area LSA Count	Area LSA Checksum
0.0.0.0	6	1	2	12	500349
0.0.0.1	6	2	2	6	200788
0.0.0.3	6	1	1	7	224952
External LSAs					
Area ID	Type	Link State ID	Router ID	Sequence	Age
0.0.0.0	Router Link	200.70.50.5	200.70.50.5	-2147483622	1305
0.0.0.0	Router Link	200.70.50.7	200.70.50.7	-2147483630	1298
0.0.0.0	Summary Link	80.0.0.0	200.70.50.5	-2147483629	1306
0.0.0.0	Summary Link	80.0.0.0	200.70.50.7	-2147483634	1303
0.0.0.0	Summary Link	100.0.0.0	200.70.50.7	-2147483632	1303

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Router ID

The VPN Concentrator OSPF router ID. This ID uniquely identifies the VPN Concentrator to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier and not an address. By convention, however, this identifier is the same as the IP address of the interface that is connected to the OSPF router network. 0 . 0 . 0 . 0 means no router is configured.

Version

The current version number of the OSPF protocol running on the VPN Concentrator.

External LSA Count

The number of external Link-State Advertisements (LSAs) in the link-state database. LSAs from neighboring OSPF Autonomous Systems (AS) describe the state of the AS router's interfaces and routing paths.

External LSA Checksum

The sum of the checksums of the external Link-State Advertisements in the link-state database. You can use this sum to determine if there has been a change in the system's OSPF router link-state database, and to compare its database with other routers.

LSAs Originated

The number of new Link-State Advertisements that the system has originated. This number is incremented each time the OSPF router originates a new LSA.

New LSAs Received

The number of Link-State Advertisements received that are completely new LSAs. This number does not include newer instances of self-originated LSAs.

LSA Database Limit

The maximum number of external LSAs that can be stored in the link-state database. A value of -1 means there is no limit.

Designated Routers

This table shows a row of statistics for each enabled VPN Concentrator interface. When OSPF routing is enabled on an interface, that interface communicates with other OSPF routers in its area, and each area elects one OSPF router to be the Designated Router.

Interface Address

The IP address of the VPN Concentrator interface that communicates with its area.

Interface Name

The VPN Concentrator interface that communicates with its area.

Ethernet 1 (Private) = Ethernet 1 (Private) interface.

Ethernet 2 (Public) = Ethernet 2 (Public) interface.

Ethernet 3 (External) = Ethernet 3 (External) interface.

WAN 1.A = WAN interface module in Slot 1, Port A

WAN 1.B = WAN interface module in Slot 1, Port B

WAN 2.A = WAN interface module in Slot 2, Port A

WAN 2.B = WAN interface module in Slot 2, Port B

Designated Router

The IP address of the Designated Router in this OSPF area.

Backup Designated Router

The IP address of the backup Designated Router in this OSPF area.

Neighbors

This table shows a row of statistics for each OSPF neighbor, for all areas in which the VPN Concentrator participates. A neighbor is another OSPF router in an OSPF area, and this table includes all such areas for the VPN Concentrator.

IP Address

The IP address of the neighboring OSPF router.

Router ID

The router ID of the neighboring OSPF router, which uniquely identifies it to other OSPF routers in its domain. While the format is that of an IP address, it functions only as an identifier. By convention, however, it is the same as the IP address of the interface that is connected to the OSPF router network.

State

The state of the relationship with this neighboring OSPF router:

Down = (Red) The VPN Concentrator has received no recent information from this neighbor. The neighbor may be out of service, or it may not have been in service long enough to establish its presence (at startup).

Initializing = The VPN Concentrator has received a Hello packet from this neighbor, but it has not yet established bidirectional communication.

Attempting = This state applies only to neighbors in an NBMA (Non-Broadcast Multi-Access) OSPF network. It indicates that the VPN Concentrator has received no recent information from this neighbor, but it is trying to establish contact by sending Hello packets at the Hello Interval.

Two Way = The VPN Concentrator has established bidirectional communication with this neighbor, but has not established adjacency; i.e., they are not exchanging routing information.

Exchange Start = The VPN Concentrator and this neighbor are in the first step of establishing an adjacency relationship.

Exchanging = The VPN Concentrator is describing its entire link state database by sending Database Description packets to this neighbor, to establish an adjacency relationship.

Loading = The VPN Concentrator is sending Link State Request packets to this neighbor asking for the more recent LSAs that have been discovered but not yet received in the Exchange state.

Full = (Green) The VPN Concentrator is in a fully adjacent relationship with this neighbor. This adjacency now appears in router LSAs and network LSAs.

Areas

This table shows a row of statistics for each OSPF Area.

Area ID

The Area ID identifies the subnet area within the OSPF Autonomous System or domain. While its format is the same as an IP address, it functions only as an identifier and not an address. 0.0.0.0 identifies a special area—the backbone—that contains all area border routers.

SPF Runs

The number of times that the system has calculated the intra-area route table (SPF, or Shortest Path First table) using this area's link-state database.

AS Border Routers

The total number of Autonomous System border routers reachable within this area.

Area Border Routers

The total number of area border routers reachable within this area.

Area LSA Count

The total number of Link-State Advertisements in this area's link-state database, excluding AS external LSAs.

Area LSA Checksum

The sum of the checksums of the Link-State Advertisements in this area's link-state database. This sum excludes external LSAs. You can use this sum to determine if there has been a change in the area's link-state database, and to compare its database with other routers.

External LSAs

This table shows a row for each external Link-State Advertisement in the link-state database.

Area ID

The Area ID identifies the Area from which the LSA was received.

Type

The LSA type. Each LSA type has a different format.

`Router Link` = Describes the states of the router's interfaces (LS Type 1).

`Network Link` = Describes the set of routers attached to the network (LS Type 2).

`Summary Link` = Describes routes to networks (LS Type 3).

`AS Summary Link` = Describes routes to AS boundary routers (LS Type 4).

`AS External Link` = Describes routes to destinations external to the AS (LS Type 5).

`Multicast Link` = Describes group membership for multicast OSPF routing (LS Type 6).

`NSSA External Link` = Describes routing for NSSAs: Not-So-Stubby-Areas (LS Type 7).

Link State ID

Either a router ID or an IP address that identifies the piece of the routing domain being described by the LSA.

Router ID

The identifier of the router in the Autonomous System that originated this LSA.

Sequence

The sequence number of this LSA. Sequence numbers are linear. They are used to detect old and duplicate LSAs. The larger the number, the more recent the LSA.

Age

The age of the LSA in seconds.

Monitor | Statistics | MIB-II | ICMP

This screen shows statistics in MIB-II objects for ICMP traffic on the VPN Concentrator since it was last booted or reset. RFC 2011 defines ICMP MIB objects.

Figure 15-45: Monitor | Statistics | MIB-II | ICMP screen

	Received	Transmitted
Total	59	13
Errors	0	0
Destination Unreachable	46	0
Time Exceeded	0	0
Parameter Problems	0	0
Source Quench	0	0
Redirects	0	0
Echo Requests (PINGs)	13	0
Echo Replies (PINGs)	0	13
Timestamp Requests	0	0
Timestamp Replies	0	0
Address Mask Requests	0	0
Address Mask Replies	0	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Received / Transmitted

The total number of ICMP messages that the VPN Concentrator received / sent. This number includes messages counted as **Errors Received / Transmitted**. ICMP messages solicit and provide information about the network environment.

Errors Received / Transmitted

The number of ICMP messages that the VPN Concentrator received but determined to have ICMP-specific errors (bad ICMP checksums, bad length, etc.).

The number of ICMP messages that the VPN Concentrator did not send due to problems within ICMP such as a lack of buffers.

Destination Unreachable Received / Transmitted

The number of ICMP Destination Unreachable messages received / sent. Destination Unreachable messages apply to many network situations, including inability to determine a route, an unusable source route specified, and the Don't Fragment flag set for a packet that must be fragmented.

Time Exceeded Received / Transmitted

The number of ICMP Time Exceeded messages received / sent. Time Exceeded messages indicate that the lifetime of the packet has expired, or that a router cannot reassemble a packet within a time limit.

Parameter Problems Received / Transmitted

The number of ICMP Parameter Problem messages received / sent. Parameter Problem messages indicate a syntactic or semantic error in an IP header.

Source Quench Received / Transmitted

The number of ICMP Source Quench messages received / sent. Source Quench messages provide rudimentary flow control; they request a reduction in the rate of sending traffic on the network.

Redirects Received / Transmitted

The number of ICMP Redirect messages received / sent. Redirect messages advise that there is a better route to a particular destination.

Echo Requests (PINGs) Received / Transmitted

The number of ICMP Echo (request) messages received / sent. Echo messages are probably the most visible ICMP messages. They test the communication path between network entities by asking for Echo Reply response messages.

Echo Replies (PINGs) Received / Transmitted

The number of ICMP Echo Reply messages received / sent. Echo Reply messages are sent in response to Echo messages, to test the communication path between network entities.

Timestamp Requests Received / Transmitted

The number of ICMP Timestamp (request) messages received / sent. Timestamp messages measure the propagation delay between network entities by including the originating time in the message, and asking for the receipt time in a Timestamp Reply message.

Timestamp Replies Received / Transmitted

The number of ICMP Timestamp Reply messages received / sent. Timestamp Reply messages are sent in response to Timestamp messages, to measure propagation delay in the network.

Address Mask Requests Received / Transmitted

The number of ICMP Address Mask Request messages received / sent. Address Mask Request messages ask for the address (subnet) mask for the LAN to which a router connects.

Address Mask Replies Received / Transmitted

The number of ICMP Address Mask Reply messages received / sent. Address Mask Reply messages respond to Address Mask Request messages by supplying the address (subnet) mask for the LAN to which a router connects.

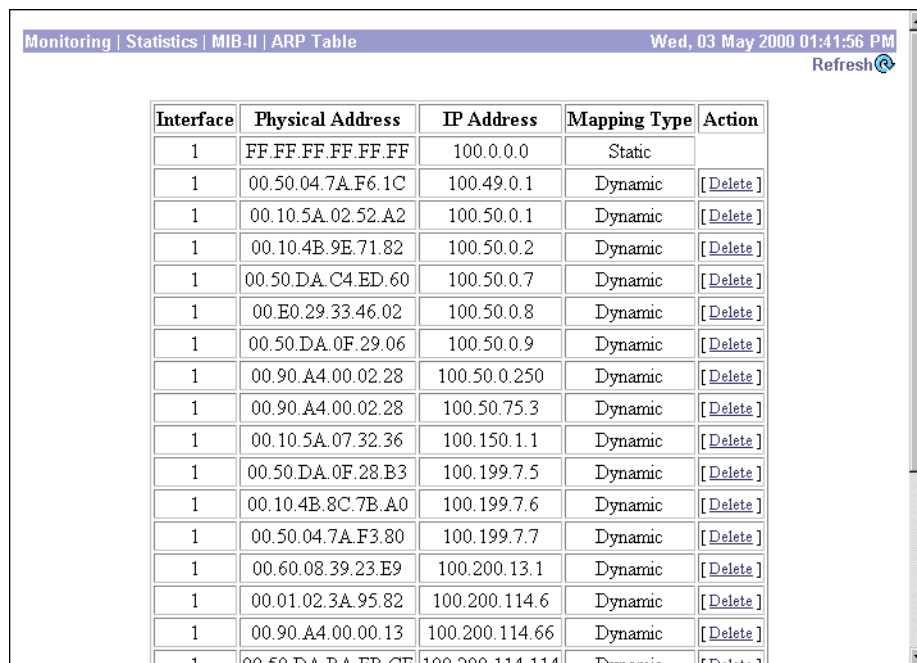
Monitor | Statistics | MIB-II | ARP Table

This screen shows entries in the Address Resolution Protocol mapping table since the VPN Concentrator was last booted or reset. ARP matches IP addresses with physical MAC addresses, so the system can forward traffic to computers on its network. RFC 2011 defines MIB entries in the ARP table.

The entries are sorted first by **Interface**, then by **IP Address**. To speed display, the Manager may construct multiple 64-row tables. Use the scroll controls (if present) to view the entire series of tables.

You can also delete dynamic, or learned, entries in the mapping table.

Figure 15-46: Monitor | Statistics | MIB-II | ARP Table screen



The screenshot shows a web browser window with the title "Monitoring | Statistics | MIB-II | ARP Table" and a timestamp "Wed, 03 May 2000 01:41:56 PM". A "Refresh" button is visible in the top right corner. The main content is a table with the following columns: Interface, Physical Address, IP Address, Mapping Type, and Action. The table contains 17 rows of data, with the first row having a static mapping and the rest being dynamic mappings with delete buttons.

Interface	Physical Address	IP Address	Mapping Type	Action
1	FF.FF.FF.FF.FF.FF	100.0.0.0	Static	
1	00.50.04.7A.F6.1C	100.49.0.1	Dynamic	[Delete]
1	00.10.5A.02.52.A2	100.50.0.1	Dynamic	[Delete]
1	00.10.4B.9E.71.82	100.50.0.2	Dynamic	[Delete]
1	00.50.DA.C4.ED.60	100.50.0.7	Dynamic	[Delete]
1	00.E0.29.33.46.02	100.50.0.8	Dynamic	[Delete]
1	00.50.DA.0F.29.06	100.50.0.9	Dynamic	[Delete]
1	00.90.A4.00.02.28	100.50.0.250	Dynamic	[Delete]
1	00.90.A4.00.02.28	100.50.75.3	Dynamic	[Delete]
1	00.10.5A.07.32.36	100.150.1.1	Dynamic	[Delete]
1	00.50.DA.0F.28.B3	100.199.7.5	Dynamic	[Delete]
1	00.10.4B.8C.7B.A0	100.199.7.6	Dynamic	[Delete]
1	00.50.04.7A.F3.80	100.199.7.7	Dynamic	[Delete]
1	00.60.08.39.23.E9	100.200.13.1	Dynamic	[Delete]
1	00.01.02.3A.95.82	100.200.114.6	Dynamic	[Delete]
1	00.90.A4.00.00.13	100.200.114.66	Dynamic	[Delete]
1	00.50.DA.BA.FB.CF	100.200.114.114	Dynamic	[Delete]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN Concentrator network interface on which this mapping applies:

- 1 = Ethernet 1 (Private) interface.
- 2 = Ethernet 2 (Public) interface.
- 3 = Ethernet 3 (External) interface.
- 8 or greater = WAN interface.
- 1000 and up = VPN tunnels, which are treated as logical interfaces.

Physical Address

The hardwired MAC (Medium Access Control) address of a physical network interface card, in 6-byte hexadecimal notation, that maps to the **IP Address**. Exceptions are:

- 00 = a virtual address for a tunnel.
- FF.FF.FF.FF.FF.FF = a network broadcast address.

IP Address

The IP address that maps to the **Physical Address**.

Mapping Type

The type of mapping:

- `Other` = none of the following.
- `Invalid` = an invalid mapping.
- `Dynamic` = a learned mapping.
- `Static` = a static mapping on the VPN Concentrator.

Action / Delete

To remove a dynamic, or learned, mapping from the table, click **Delete**. *There is no confirmation or undo.* The Manager deletes the entry and refreshes the screen.

To delete an entry, you must have the administrator privilege to **Modify Config** under **General Access Rights**. See **Administration | Access Rights | Administrators**.


You cannot delete static mappings.

Monitor | Statistics | MIB-II | Ethernet

This screen shows statistics in MIB-II objects for Ethernet interface traffic on the VPN Concentrator since it was last booted or reset. IEEE standard 802.3 describes Ethernet networks, and RFC 1650 defines Ethernet interface MIB objects.

To configure Ethernet interfaces, see [Configuration | Interfaces](#).

Figure 15-47: Monitor | Statistics | MIB-II | Ethernet screen

Monitoring Statistics MIB-II Ethernet														Mon, 22 May 2000 04:34:48 PM	
														Refresh 	
Interface	Errors					Deferred Transmits	Collisions				MAC Errors		Speed (Mbps)	Duplex	
	Alignment	FCS	Carrier Sense	SQE Test	Frame Too Long		Single	Multiple	Late	Excessive	Transmit	Receive			
Ethernet 1 (Private)	0	0	0	0	0	0	0	0	0	0	0	0	0	100	Half
Ethernet 2 (Public)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Half

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The Ethernet interface to which the data in this row applies. Only configured interfaces are shown.

Alignment Errors

The number of frames received on this interface that are not an integral number of bytes long and do not pass the FCS (Frame Check Sequence; used for error detection) check.

FCS Errors

The number of frames received on this interface that are an integral number of bytes long but do not pass the FCS (Frame Check Sequence) check.

Carrier Sense Errors

The number of times that the carrier sense signal was lost or missing when trying to transmit a frame on this interface.

SQE Test Errors

The number of times that the SQE (Signal Quality Error) Test Error message was generated for this interface. The SQE message tests the collision circuits on an interface.

Frame Too Long Errors

The number of frames received on this interface that exceed the maximum permitted frame size.

Deferred Transmits

The number of frames for which the first transmission attempt on this interface is delayed because the medium is busy. This number does not include frames involved in collisions.

Single Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by exactly one collision. This number is not included in the **Multiple Collisions** number.

Multiple Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by more than one collision. This number does not include the **Single Collisions** number.

Late Collisions

The number of times that a collision is detected on this interface later than 512 bit-times into the transmission of a packet. 512 bit-times = 51.2 microseconds on a 10-Mbps system.

Excessive Collisions

The number of frames for which transmission on this interface failed due to excessive collisions.

MAC Errors: Transmit

The number of frames for which transmission on this interface failed due to an internal MAC sublayer transmit error. This number does not include **Carrier Sense Errors**, **Late Collisions**, or **Excessive Collisions**.

MAC Errors: Receive

The number of frames for which reception on this interface failed due to an internal MAC sublayer receive error. This number does not include **Alignment Errors**, **FCS Errors**, or **Frame Too Long Errors**.

Speed (Mbps)

This interface's nominal bandwidth in megabits per second.

Duplex

The current LAN duplex transmission mode for this interface:

`Full` = Full-Duplex: transmission in both directions at the same time.

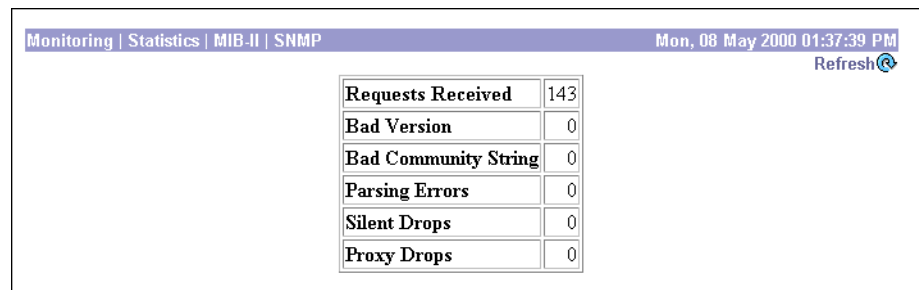
`Half` = Half-Duplex: transmission in only one direction at a time.

Monitor | Statistics | MIB-II | SNMP

This screen shows statistics in MIB-II objects for SNMP traffic on the VPN Concentrator since it was last booted or reset. RFC 1907 defines SNMP version 2 MIB objects.

To configure the VPN Concentrator SNMP server, see **Configuration | System | Management Protocols | SNMP**.

Figure 15-48: Monitor | Statistics | MIB-II | SNMP screen



The screenshot shows a web interface with a navigation bar at the top containing "Monitoring | Statistics | MIB-II | SNMP" and a timestamp "Mon, 08 May 2000 01:37:39 PM" with a "Refresh" button. Below the navigation bar is a table with the following data:

Requests Received	143
Bad Version	0
Bad Community String	0
Parsing Errors	0
Silent Drops	0
Proxy Drops	0

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests Received

The total number of SNMP messages received by the VPN Concentrator.

Bad Version

The total number of SNMP messages received that were for an unsupported SNMP version. The VPN Concentrator supports SNMP version 2.

Bad Community String

The total number of SNMP messages received that used an SNMP community string the VPN Concentrator did not recognize. See **Configuration | System | Management Protocols | SNMP Communities** to configure permitted community strings. To protect security, the VPN Concentrator *does not* include the usual default `public` community string.

Parsing Errors

The total number of syntax or transmission errors encountered by the VPN Concentrator when decoding received SNMP messages.

Silent Drops

The total number of SNMP request messages that were silently dropped because the reply exceeded the maximum allowable message size.

Proxy Drops

The total number of SNMP request messages that were silently dropped because the transmission of the reply message to a proxy target failed for some reason (other than a timeout).

End of Chapter



Using the Command Line Interface

The VPN 3000 Concentrator Series Command Line Interface (CLI) is a menu- and command-line-based configuration, administration, and monitoring system built into the VPN Concentrator. You use it via the system console or a Telnet (or Telnet over SSL) session.

You can use the CLI to completely manage the system. You can access and configure the same parameters as the HTML-based VPN 3000 Concentrator Series Manager, except for IPSec LAN-to-LAN configuration.

This chapter describes general features of the CLI and how to access and use it. It *does not* describe the individual menu items and parameter entries. For information on specific parameters and options, see the corresponding section of the VPN Concentrator Manager in this manual. For example, to understand Ethernet interface configuration parameters and choices, see **Configuration | Interfaces | Ethernet 1 2 3** in Chapter 3, *Interfaces*.

Accessing the CLI

You can access the CLI in two ways: via the system console or a Telnet (or Telnet over SSL) client.

Console access

To access the CLI via console:

- 1 Connect a PC to the VPN Concentrator via a straight-through RS-232 serial cable (which Cisco supplies with the system) between the **Console** port on the VPN Concentrator and the COM1 or serial port on the PC. For more information, see the *VPN Concentrator Getting Started* manual.
- 2 Start a terminal emulator (e.g., HyperTerminal) on the PC. Configure a connection to COM1 with port settings of:
 - 9600 bits per second.
 - 8 data bits.
 - No parity.
 - 1 stop bit.
 - Hardware flow control.Set the emulator for VT100 emulation, or let it auto-detect the emulation type.

- 3 Press **Enter** on the PC keyboard until you see the login prompt. (You may see a password prompt and error messages as you press **Enter**; ignore them and stop at the login prompt.)

Login: _

Telnet or Telnet/SSL access

To access the CLI via a Telnet or Telnet/SSL client:

- 1 Enable the Telnet or Telnet/SSL server on the VPN Concentrator. (They are both enabled by default.) See the **Configuration | System | Management Protocols | Telnet** screen on the VPN Concentrator Manager.

- 2 Start the Telnet or Telnet/SSL client, and connect to the remote system using these parameters:

Host Name or **Session Name** = The IP address on the VPN Concentrator Ethernet 1 (Private) interface; e.g., 10.10.147.2

Port = Telnet (default Telnet port is 23, Telnet/SSL port is 992)

Terminal Type = VT100 or ANSI

Telnet/SSL only: If the client offers it, enable *both* **SSL** and **SSL Only**.

- 3 The VPN Concentrator displays a login prompt.

Login: _

Starting the CLI

You start the CLI by logging in.

CLI login usernames and passwords for both console and Telnet access are the same as those configured and enabled for administrators. See the **Administration | Access Rights | Administrators** screen. By default, only admin is enabled.

This example uses the factory-supplied default admin login and password. If you have changed them, use your entries.

At the prompts, enter the administrator login name and password. Entries are case-sensitive.

Login: admin

Password: admin (The CLI does not show your entry.)

The CLI displays the opening welcome message, the main menu, and the Main -> prompt.

```
                Welcome to
                Cisco Systems
                VPN 3000 Concentrator Series
                Command Line Interface
                Copyright (C) 1998-2000 Cisco Systems, Inc.
```

- ```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

Main -> \_

## Using the CLI

This section explains how to:

- Choose menu items.
- Enter values for parameters and options.
- Specify configured items by number or name.
- Navigate quickly—using shortcuts—through the menus.
- Display a brief help message.
- Save entries to the system configuration file.
- Stop the CLI.
- Understand CLI administrator access rights.

The CLI displays menus or prompts at every level to guide you in choosing configurable options and setting parameters. The prompt always shows the menu context.

### Choosing menu items

To use the CLI, enter a number at the prompt that corresponds to the desired menu item, and press **Enter**.

For example, this is the **Configuration > System > General > System Identification** menu:

- 1) Set System Name
- 2) Set Contact
- 3) Set Location
- 4) Back

```
General -> _
```

Enter 1 to set the system name.

### Entering values

The CLI shows any current or default value for a parameter in brackets [ ]. To change the value, enter a new value at the prompt. To leave the value unchanged, just press **Enter**.

Continuing the example above, this is the prompt to enter a value for the system name:

```
> Host Name
```

```
General -> [Lab VPN] _
```

You can enter a new name at the prompt, or just press **Enter** to keep the current name.

## Specifying configured items

Many menus give choices that act on configured items—such as groups, users, filter rules, etc.—and the CLI lists those items with a number and their name. To specify an item, you can usually enter either its number or its name. The CLI indicates when you must use a specific identifier (usually the item’s number).

For example, the **Configuration > User Management > Groups** menu lists configured groups:

```
Current User Groups

| 1. QuickGroup | 2. IPSecGroup

```

- 1) Add a Group
- 2) Modify a Group
- 3) Delete a Group
- 4) Back

Groups -> \_

To delete QuickGroup, enter 3 at the prompt. The CLI displays:

```
> Enter the Group to Delete
```

Groups -> \_

At the prompt you can enter either its number (1) or its name (QuickGroup).

However, this next example shows the prompt for a specific identifier. The **Configuration > System > Servers > Authentication** menu lists configured servers:

Authentication Server Summary Table

| Num | Server        | Type     | Port |
|-----|---------------|----------|------|
| 1   | Internal      | Internal | 0    |
| 2   | 192.168.34.56 | RADIUS   | 0    |

- 1) Add Authentication Server
- 2) Modify Authentication Server
- 3) Delete Authentication Server
- 4) Move Server Up
- 5) Move Server Down
- 6) Test Server
- 7) Back

Authentication -> \_

To delete the RADIUS server, enter 3 at the prompt. The CLI displays:

```
> Delete Server (number)
```

Authentication -> \_

At the prompt, you must enter 2 for the RADIUS server.



## Navigating quickly through the CLI

There are two ways to move quickly through the CLI: shortcut numbers, and the Back/Home options. Both ways work only when you are at a menu, not when you are at a value entry.

### Using shortcut numbers

Once you become familiar with the structure of the CLI—which parallels the HTML-based VPN Concentrator Manager—you can quickly access any level by entering a series of numbers separated by periods. For example, suppose you want to change the General Parameters for the Base Group. The series of menus that gets to that level from the main menu is:

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 1 (Configuration)

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

Config -> 3 (User Management)

- 1) Base Group
- 2) Groups
- 3) Users
- 4) Back

User Management -> 1 (Base Group)

- 1) General Parameters
- 2) Server Parameters
- 3) IPSec Parameters
- 4) PPTP/L2TP Parameters
- 5) Back

Base Group -> 1 (General Parameters)

- 1) Access Parameters
- 2) Tunneling Protocols
- 3) SEP Config
- 4) Back

Base Group -> \_

As a shortcut, you can just enter 1.3.1.1 at the Main-> prompt, and move directly to the Base Group General Parameters menu:

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 1.3.1.1

- 1) Access Parameters
- 2) Tunneling Protocols
- 3) SEP Config
- 4) Back

Base Group -> \_

The prompt always shows the current context in the menu structure.

### Using Back and Home

Most menus include a numbered Back choice. Instead of entering a number, you can just enter b or B to move back to the previous menu.

Also, at any menu level, you can just enter h or H to move home to the main menu.

### Getting Help Information

To display a brief help message, enter 5 at the main menu prompt. The CLI explains how to navigate through menus and enter values. This help message is available only at the main menu.

```
Cisco Systems. Help information for the Command Line Interface
```

```
From any menu except the Main menu.
-- 'B' or 'b' for Back to previous menu.
-- 'H' or 'h' for Home back to the main menu.
```

```
For Data entry
-- Current values are in '[']'s. Just hit 'Enter' to accept value.
```

- 1) View Help Again
- 2) Back

```
Help -> _
```

To return to the main menu from this help menu, enter h (for home), or 2 or b (for back) at the prompt.

## Saving the configuration file

Configuration and administration entries take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN Concentrator without *saving* the active configuration, you lose any changes.

To save changes to the system configuration (CONFIG) file, navigate to the main menu. At the prompt, enter 4 for Save changes to Config file.

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> 4
```

The system writes the active configuration to the CONFIG file and redisplay the main menu.

## Stopping the CLI

To stop the CLI, navigate to the main menu and enter 6 for Exit at the prompt:

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> 6
```

```
Done
```

Make sure you save any configuration changes before you exit from the CLI.

## Understanding CLI access rights

What you see and can configure with the CLI depends on administrator access rights. If you don't have permission to configure an option, you see -), rather than a number, in menus.

For example, here is the main menu for the default User administrator:

- ) Configuration
- ) Administration
- 3) Monitoring
- ) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main -> _
```

The default User administrator can only monitor the VPN Concentrator, not configure system parameters or administer the system.

See **Administration | Access Rights | Administrators** in Chapter 14, *Administration*, for more information.

# CLI menu reference

This section shows all the menus in the first three levels below the CLI main menu. (There are many additional menus below the third level; and within the first three levels, there are some non-menu parameter settings. To keep this chapter at a reasonable size, we show only the *menus* here.)

The numbers in each heading are the keyboard shortcut to reach that menu from the main menu. For example, entering 1 . 3 . 1 at the main menu prompt takes you to the **Configuration > User Management> Base Group** menu.

---

**Notes:** The CLI menus and options—and thus the keyboard shortcuts—may change with new software versions. Please check familiar shortcuts carefully when using a new release.

The Model 3005 has two Ethernet interfaces and one expansion card slot, and Models 3015–3080 have three interfaces and four expansion card slots. Therefore, CLI menu shortcuts differ where they involve interface and expansion card selections. We note some differences here, but please note carefully the system you are using.

---

## Main menu

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> \_

## 1 Configuration

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

Config -> \_

## 1.1 Configuration > Interface Configuration

This table shows current IP addresses.

.  
.  
.

*Model  
3015–3080 only*

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Configure Expansion Cards
- 6) Back

Interfaces -> \_

*Model 3005 only*

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Power Supplies
- 4) Configure Expansion Cards
- 5) Back

Interfaces -> \_

### 1.1.1, 1.1.2, or 1.1.3 Configuration > Interface Configuration > Configure Ethernet #1 or #2 or #3

*Only 1.1.1 and 1.1.2  
on Model 3005*

- 1) Enable/Disable
- 2) Set IP Address
- 3) Set Subnet Mask
- 4) Select IP Filter
- 5) Select Ethernet Speed
- 6) Select Duplex
- 7) Set Port Routing Config
- 8) Set Public Interface
- 9) Back

Ethernet Interface 1 -> \_

### 1.1.4 Configuration > Interface Configuration > Configure Power Supplies

*Model  
3015–3080 only*

Alarm Thresholds in centivolts (e.g. 361 = 3.61V)  
Voltages will be adjusted to conform to the hardware.

- 1) Configure CPU voltage thresholds
- 2) Configure Power Supply 1 voltage thresholds
- 3) Configure Power Supply 2 voltage thresholds
- 4) Configure Board voltage thresholds
- 5) Back

Interfaces -> \_

## 1.1.3 Configuration > Interface Configuration > Configure Power Supplies

*Model 3005 only* Alarm Thresholds in centivolts (e.g. 361 = 3.61V)  
Voltages will be adjusted to conform to the hardware.

- 1) Configure CPU voltage thresholds
- 2) Configure Power Supply voltage thresholds
- 3) Configure Board voltage thresholds
- 4) Back

Interfaces -> \_

## 1.1.5 Configuration > Interface Configuration > Configure Expansion Cards

*Model  
3015-3080 only*

| Expansion Cards |      |    |                |
|-----------------|------|----|----------------|
| -----           |      |    |                |
| 1.              | SEP  | 2. | Dual T1/E1 WAN |
| -----           |      |    |                |
| 3.              | None | 4. | None           |
| -----           |      |    |                |

- 1) Configure Slot #1
- 2) Configure Slot #2
- 3) Configure Slot #3
- 4) Configure Slot #4
- 5) Back

Interfaces -> \_

## 1.1.4 Configuration > Interface Configuration > Configure Expansion Cards

*Model 3005 only* Expansion Card:

- 1) Configure Expansion Card
- 2) Back

Interfaces -> \_

## 1.2 Configuration > System Management

- 1) Servers (Authentication, Accounting, etc.)
- 2) Address Management
- 3) Tunneling Protocols (PPTP, L2TP, etc.)
- 4) IP Routing (static routes, OSPF, etc.)
- 5) Management Protocols (Telnet, TFTP, FTP, etc.)
- 6) Event Configuration
- 7) General Config (system name, time, etc.)
- 8) Back

System -> \_

## 1.2.1 Configuration > System Management > Servers

- 1) Authentication Servers
- 2) Accounting Servers
- 3) DNS Servers
- 4) DHCP Servers
- 5) NTP Servers
- 6) Back

Servers -> \_

## 1.2.2 Configuration > System Management > Address Management

- 1) Address Assignment
- 2) Address Pools
- 3) Back

Address -> \_

## 1.2.3 Configuration > System Management > Tunneling Protocols

- 1) PPTP
- 2) L2TP
- 3) IKE Proposals
- 4) Back

Tunnel -> \_

---

**Note:** The CLI does not include IPSec LAN-to-LAN configuration.

---

## 1.2.4 Configuration > System Management > IP Routing

- 1) Static Routes
- 2) Default Gateways
- 3) OSPF
- 4) OSPF Areas
- 5) DHCP
- 6) Redundancy
- 7) Back

Routing -> \_

### 1.2.5 Configuration > System Management > Management Protocols

```
Network Protocol Summary Table
.
.
.

1) Configure FTP
2) Configure HTTP/HTTPS
3) Configure TFTP
4) Configure Telnet
5) Configure SNMP
6) Configure SNMP Community Strings
7) Configure SSL
8) Back

Network -> _
```

### 1.2.6 Configuration > System Management > Event Configuration

```
1) General
2) FTP Backup
3) Classes
4) Trap Destinations
5) Syslog Servers
6) SMTP Servers
7) Email Recipients
8) Back

Event -> _
```

### 1.2.7 Configuration > System Management > General Config

```
1) System Identification
2) System Time and Date
3) Back

General -> _
```

### 1.3 Configuration > User Management

```
1) Base Group
2) Groups
3) Users
4) Back

User Management -> _
```



### 1.3.1 Configuration > User Management > Base Group

- 1) General Parameters
- 2) Server Parameters
- 3) IPSec Parameters
- 4) PPTP/L2TP Parameters
- 5) Back

Base Group -> \_

### 1.3.2 Configuration > User Management > Groups

Current User Groups

- .
- .
- .
- 1) Add a Group
- 2) Modify a Group
- 3) Delete a Group
- 4) Back

Groups -> \_

### 1.3.3 Configuration > User Management > Users

Current Users

- .
- .
- .
- 1) Add a User
- 2) Modify a User
- 3) Delete a User
- 4) Back

Users -> \_

### 1.4 Configuration > Policy Management

- 1) Access Hours
- 2) Traffic Management
- 3) Back

Policy -> \_

### 1.4.1 Configuration > Policy Management > Access Hours

```
Current Access Hours
.
.
.
1) Add Access Hours
2) Modify Access Hours
3) Delete Access Hours
4) Back

Access Hours -> _
```

### 1.4.2 Configuration > Policy Management > Traffic Management

```
1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT)
6) Back

Traffic -> _
```

## 2 Administration

```
1) Administer Sessions
2) Software Update
3) System Reboot
4) Ping
5) Access Rights
6) File Management
7) Certificate Management
8) Back

Admin -> _
```

### 2.1 Administration > Administer Sessions

```
Active Sessions
.
.
.
1) Refresh Session Status
2) Logoff Session
3) Session Details
4) Back

Admin -> _
```

## 2.3 Administration > System Reboot

- 1) Cancel Scheduled Reboot/Shutdown
- 2) Schedule Reboot
- 3) Schedule Shutdown
- 4) Back

Admin -> \_

### 2.3.2 Administration > System Reboot > Schedule Reboot

- 1) Save active Configuration and use it at Reboot
- 2) Reboot without saving active Configuration file
- 3) Reboot with Factory/Default Configuration
- 4) Back

Admin -> \_

### 2.3.3 Administration > System Reboot > Schedule Shutdown

- 1) Save active configuration and use it at next reboot
- 2) Shutdown without saving active Configuration file
- 3) Use Factory/Default Configuration at next reboot
- 4) Back

Admin -> \_

## 2.5 Administration > Access Rights

- 1) Administrators
- 2) Access Control List
- 3) Access Settings
- 4) Back

Admin -> \_

### 2.5.1 Administration > Access Rights > Administrators

Administrative Users

.  
.  
.

- 1) Modify Administrator
- 2) Back

Admin -> \_

### 2.5.2 Administration > Access Rights > Access Control List

```
This is the Current Access List
.
.
.
1) Add Manager Workstation
2) Modify Manager Workstation
3) Delete Manager Workstation
4) Move Manager Workstation Up
5) Move Manager Workstation Down
6) Back

Admin -> _
```

### 2.5.3 Administration > Access Rights > Access Settings

```
1) Set Session Timeout
2) Set Session Limit
3) Enable/Disable Encrypt Config File
4) Back

Admin -> _
```

### 2.6 Administration > File Management

```
List of Files
.
.
.
1) Delete File
2) Copy File
3) View File
4) Put File via TFTP
5) Get File via TFTP
6) Swap Configuration File
7) Upload Configuration File
8) Back

File -> _
```

### 2.6.6 Administration > File Management > Swap Configuration File

```
Every time the active configuration is saved,...
.
.
.
1) Swap
2) Back

Admin -> _
```

## 2.7 Administration > Certificate Management

- 1) Enrollment
- 2) Installation
- 3) Certificate Authorities
- 4) Identity Certificates
- 5) SSL Certificate
- 6) Back

Certificates -> \_

### 2.7.2 Administration > Certificate Management > Installation

- 1) Install Certificate Authority
- 2) Install SSL Certificate (from Enrollment)
- 3) Install SSL Certificate (with private key)
- 4) Install Identity Certificate (from Enrollment)
- 5) Install Identity Certificate (with private key)
- 6) Back

Certificates -> \_

### 2.7.3 Administration > Certificate Management > Certificate Authorities

Certificate Authorities

- .
- .
- .
- 1) View Certificate
- 2) Delete Certificate
- 3) CRL Configuration
- 4) Back

Certificates -> \_

### 2.7.4 Administration > Certificate Management > Identity Certificates

Identity Certificates

- .
- .
- .
- 1) View Certificate
- 2) Delete Certificate
- 3) Back

Certificates -> \_

### 2.7.5 Administration > Certificate Management > SSL Certificate

```
Subject
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
Issuer
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
Serial Number
.
.

1) Delete Certificate
2) Generate Certificate
3) Back

Certificates -> _
```

## 3 Monitoring

```
1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Back

Monitor -> _
```

### 3.1 Monitoring > Routing Table

```
Routing Table
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
.
1) Refresh Routing Table
2) Back

Routing -> _
```

## 3.2 Monitoring > Event Log

- 1) Configure Log viewing parameters
- 2) View Event Log
- 3) Save Log
- 4) Clear Log
- 5) Back

Log -> \_

### 3.2.2 Monitoring > Event Log > View Event Log

[Event Log entries]

- .
- .
- .
- 1) First Page
  - 2) Previous Page
  - 3) Next Page
  - 4) Last Page
  - 5) Back

Log -> \_

## 3.3 Monitoring > System Status

System Status

- .
- .
- .
- 1) Refresh System Status
  - 2) View Card Status
  - 3) Back

Status -> \_

### 3.3.2 Monitoring > System Status > View Card Status

*Model  
3015–3080 only*

- 1) Card in Slot 1
- 2) Card in Slot 2
- 3) Card in Slot 3
- 4) Card in Slot 4
- 5) Back

Card Status -> \_

*Model 3005 only*

- 1) Card in Slot 1
- 2) Back

Card Status -> \_

### 3.4 Monitoring > Sessions

*Model  
3015–3080 only*

- 1) View Session Statistics
- 2) View Top Ten Lists
- 3) View Session Protocols
- 4) View Session SEPs
- 5) View Session Encryption
- 6) Back

Sessions -> \_

*Model 3005 only*

- 1) View Session Statistics
- 2) View Top Ten Lists
- 3) View Session Protocols
- 4) View Session Encryption
- 5) Back

Sessions -> \_

#### 3.4.1 Monitoring > Sessions > View Session Statistics

Active Sessions  
.  
.  
.  
1) Refresh Session Statistics  
2) Session Details  
3) Back

Sessions -> \_

#### 3.4.2 Monitoring > Sessions > View Top Ten Lists

- 1) Top 10 Users based on Data
- 2) Top 10 Users based on Duration
- 3) Top 10 Users based on Throughput
- 4) Back

Sessions -> \_

#### 3.4.3 Monitoring > Sessions > View Session Protocols

Session Protocols  
.  
.  
.  
1) Refresh Session Protocols  
2) Back

Sessions -> \_



### 3.4.4 Monitoring > Sessions > View Session SEPs

```

Model
3015-3080 only Session SEPs
 .
 .
 .

 1) Refresh Session SEPs
 2) Back

Sessions -> _

```

### 3.4.5\* Monitoring > Sessions > View Session Encryption

```

* 3.4.5 on Model Session Encryption
3015-3080,
3.4.4 on Model .
3005 .
 .

 1) Refresh Session Encryption
 2) Back

Sessions -> _

```

### 3.5 Monitoring > General Statistics

```

 1) Protocol Statistics
 2) Server Statistics
 3) Event Statistics
 4) MIB II Statistics
 5) Back

General -> _

```

#### 3.5.1 Monitoring > General Statistics > Protocol Statistics

```

 1) PPTP Statistics
 2) L2TP Statistics
 3) IPSec Statistics
 4) HTTP Statistics
 5) Telnet Statistics
 6) DNS Statistics
 7) VRRP Statistics
 8) SSL Statistics
 9) Back

General -> _

```

### 3.5.2 Monitoring > General Statistics > Server Statistics

- 1) Authentication Statistics
- 2) Accounting Statistics
- 3) Filtering Statistics
- 4) DHCP Statistics
- 5) Address Pool Statistics
- 6) Back

General -> \_

### 3.5.3 Monitoring > General Statistics > Event Statistics

```
Event Statistics
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
.
1) Refresh Event Statistics
2) Back
```

General -> \_

### 3.5.4 Monitoring > General Statistics > MIB II Statistics

- 1) Interface-based
- 2) System-level
- 3) Back

MIB2 -> \_

**End of Chapter**



## Errors and troubleshooting

---

This appendix describes common errors that may occur while configuring and using the system, and how to correct them. It also describes LED indicators on the system and its expansion modules.

### Files for troubleshooting

The VPN 3000 Concentrator creates several files that you can examine, and that can assist Cisco support engineers, when troubleshooting errors and problems:

- Event log.
- `SAVELOG.TXT` = Event log that is automatically saved when the system crashes and when it is rebooted.
- `CRSHDUMP.TXT` = Internal system data file that is written when the system crashes.
- `CONFIG`, `CONFIG.BAK` = Normal configuration file used to boot the system, and backup configuration file.

### Event logs

The VPN Concentrator records system events in the event log, which is stored in nonvolatile memory (NVRAM). To troubleshoot operational problems, we recommend that you start by examining the event log. See **Configuration | System | Events** and **Monitor | Event Log**.

The VPN Concentrator automatically saves the event log to a file in flash memory if it crashes, and when it is rebooted. This log file is named `SAVELOG.TXT`, and it overwrites any existing file with that name. The `SAVELOG.TXT` file is useful for debugging. See **Configuration | System | Events** and **Administration | File Management | Files**.

### Crash dump file

If the VPN Concentrator crashes during operation, it saves internal system data in nonvolatile memory (NVRAM), and then automatically writes this data to a `CRSHDUMP.TXT` file in flash memory when it is rebooted. This file contains the crash date and time, software version, tasks, stack, registers, memory, buffers, timers, etc., which are helpful to Cisco support engineers. In case of a crash, we ask that you send this file when you contact Cisco for assistance. See **Administration | File Management | Files** for information on managing files in flash memory.

### Configuration files

The VPN Concentrator saves the current boot configuration file (CONFIG) and its predecessor (CONFIG.BAK) as files in flash memory. These files may be useful for troubleshooting. See **Administration | File Management | Files** for information on managing files in flash memory.

### VPN Concentrator Manager errors

These errors may occur while using the HTML-based VPN Concentrator Manager with a browser.

#### Browser Refresh / Reload button logs out the Manager

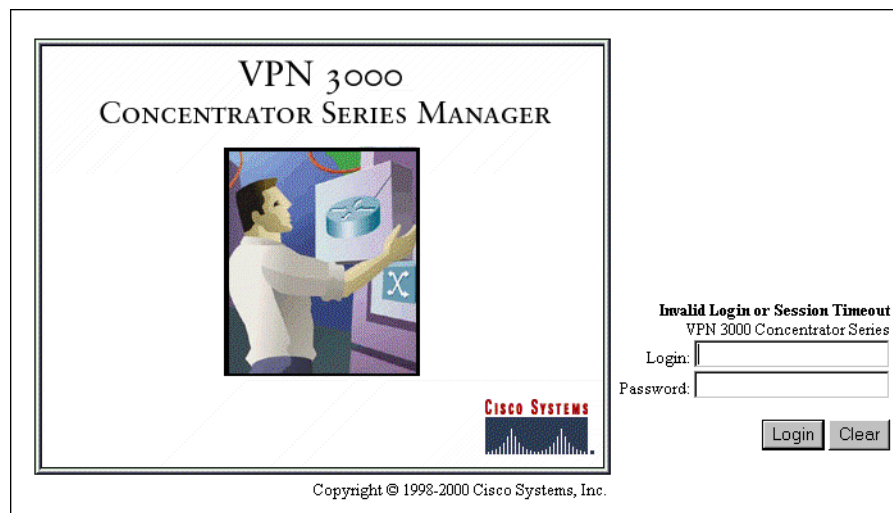
| Problem                                                                                                                                                       | Possible cause                                                                                                                                                                    | Solution                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked the <b>Refresh</b> or <b>Reload</b> button on the <i>browser's</i> navigation toolbar, and the Manager logged out. The main login screen appears. | <ul style="list-style-type: none"><li>To protect access security, clicking <b>Refresh / Reload</b> on the browser's toolbar automatically logs out the Manager session.</li></ul> | <p>Do not use the browser's navigation toolbar buttons with the VPN Concentrator Manager.</p> <p>Use only the Manager's <b>Refresh</b> button where it appears on a screen.</p> <p>We recommend that you hide the browser's navigation toolbar to prevent mistakes.</p> |

#### Browser Back or Forward button displays an incorrect screen or incorrect data

| Problem                                                                                                                                                        | Possible cause                                                                                                                                                                                                         | Solution                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked the <b>Back</b> or <b>Forward</b> button on the <i>browser's</i> navigation toolbar, and the Manager displayed the wrong screen or incorrect data. | <ul style="list-style-type: none"><li>To protect security and the integrity of data entries, clicking <b>Back</b> or <b>Forward</b> on the browser's toolbar deletes pointers and values within the Manager.</li></ul> | <p>Do not use the browser's navigation toolbar buttons with the VPN Concentrator Manager.</p> <p>Navigate using the location bar at the top of the Manager window, the table of contents in the left frame, or links on Manager screens.</p> <p>We recommend that you hide the browser's navigation toolbar to prevent mistakes.</p> |

## Invalid Login or Session Timeout

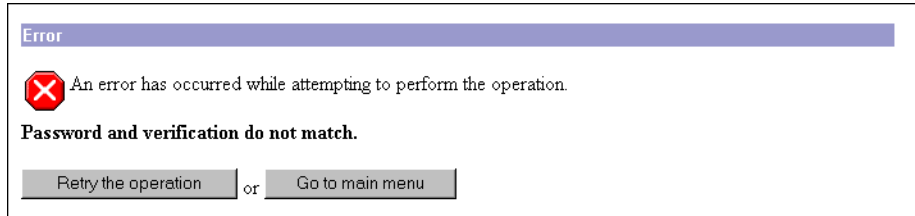
The Manager displays the **Invalid Login or Session Timeout** screen



| Problem                                                                        | Possible cause                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Solution                                                                                                                                                     |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You entered an invalid administrator login name / password combination.        | <ul style="list-style-type: none"> <li>• Typing error.</li> <li>• Invalid (unrecognized) login name or password.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                               | Re-enter the login name and password, and click the <b>Login</b> button. Use a valid login name and password. Type carefully.                                |
| The Manager session has been idle longer than the configured timeout interval. | <ul style="list-style-type: none"> <li>• No activity for (interval) seconds. The Manager resets the inactivity timer only when you click an action button (<b>Apply</b>, <b>Add</b>, <b>Cancel</b>, etc.) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen <i>does not</i> reset the timer.</li> <li>• Default timeout interval is 600 seconds (10 minutes).</li> <li>• Timeout interval set too low for normal use.</li> </ul> | On the <b>Administration   Access Rights   Access Settings</b> screen, change the <b>Session Timeout</b> interval to a larger value and click <b>Apply</b> . |

### Error / An error has occurred while attempting to perform...

The Manager displays a screen with the message: **Error / An error has occurred while attempting to perform the operation**. An additional error message describes the erroneous operation.



---

| Problem                                                  | Possible cause                                                                                          | Solution                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You tried to perform some operation that is not allowed. | <ul style="list-style-type: none"><li>The screen displays a message that describes the cause.</li></ul> | Click <b>Retry the operation</b> to return to the screen where you were working and correct the mistake. <i>Carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost.</i><br><br>Click <b>Go to main menu</b> to go to the main Manager screen. |

---

## You are using an old browser or have disabled JavaScript

The Manager displays a screen with the message: **You are using an old browser or have disabled JavaScript...**

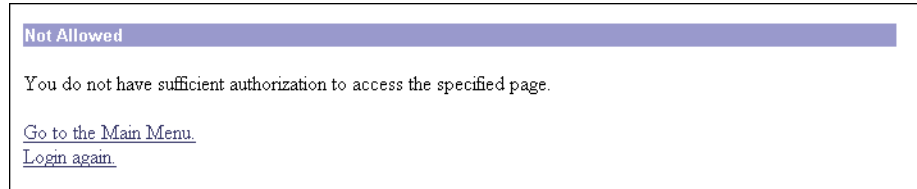
### VPN 3000 Concentrator Series

You are using an old browser or have disabled JavaScript. You **must** use version 4 or higher of Netscape Navigator/Communicator or version 4 or higher of Microsoft Internet Explorer with JavaScript enabled.

| Problem                                                                          | Possible cause                                                                                                                                                                                                                            | Solution                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The VPN Concentrator Manager cannot work with the browser that you have invoked. | <ul style="list-style-type: none"><li>You are using the Manager with an unsupported browser.</li><li>You are using the Manager with an obsolete browser.</li><li>You are using a browser that does not have JavaScript enabled.</li></ul> | <p>Use Microsoft Internet Explorer version 4.0 or higher.</p> <p>Use Netscape Communicator or Navigator version 4.0 or higher.</p> <p>Be sure JavaScript is enabled in the browser. See <i>Required browser</i> in Chapter 2 of <i>VPN 3000 Concentrator Series Getting Started</i>, or <i>Browser requirements</i> in Chapter 1 of <i>VPN 3000 Concentrator Series User Guide</i>.</p> |

## Not Allowed / You do not have sufficient authorization...

The Manager displays a screen with the message: **Not Allowed / You do not have sufficient authorization to access the specified page.**




| Problem                                                                                  | Possible cause                                                                                                                                                                                            | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You tried to access an area of the Manager that you do not have authorization to access. | <ul style="list-style-type: none"><li>You logged in using an administrator login name that has limited privileges.</li><li>You logged in from a workstation that has limited access privileges.</li></ul> | <p>Log in using the system administrator login name and password. (Defaults are admin / admin.)</p> <p>Log in from a workstation with greater access privileges.</p> <p>Have the system administrator change your privileges on the <b>Administration   Access Rights   Administrators</b> screen.</p> <p>Have the system administrator change the privileges of your workstation on the <b>Administration   Access Rights   Access Control List</b> screen.</p> |



## Not Found / An error has occurred while attempting to access...

The Manager displays a screen with the message: **Not Found / An error has occurred while attempting to access the specified page.** The screen includes additional information that identifies system activity and parameters.

**Not Found**



An error has occurred while attempting to access the specified page. The feature hasn't been implemented yet, or the page does not exist. If you have recently upgraded or downgraded the VPN 3000 Concentrator Series, clearing the browser's cache may solve the problem.

**Error:** HTTP 404 - Not Found  
**Request:** GET http://10.10.147.2/foobar.html  
**Referring Page:** Unknown  
**Browser:** Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)  
**JavaScript:** JavaScript 1.2  
**Software Version:** Cisco Systems, Inc./VPN 3000 Concentrator Series Version 2.5 (6898) built by tshorn on Apr 14 2000 13:55:31 (DEBUG\_MASK 0, NDEBUG off)  
**Feature Set:**

[Go to the login page.](#)

| Problem                              | Possible cause                                                                                                          | Solution                                                                                                                    |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| The Manager could not find a screen. | <ul style="list-style-type: none"> <li>You updated the software image and did not clear the browser's cache.</li> </ul> | Clear the browser's cache: delete its temporary internet files, history files, and location bar references. Then try again. |
|                                      | <ul style="list-style-type: none"> <li>There is an internal Manager error.</li> </ul>                                   | Please note the system information on the screen and contact Cisco support personnel for assistance.                        |

## Microsoft Internet Explorer Script Error: No such interface supported

Microsoft Internet Explorer displays a Script Error dialog box that includes the error message: **No such interface supported.**

| Problem                                                                                                                                                                                                  | Possible cause                                                                                           | Solution                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| While using a Manager function that opens another browser window (such as <b>Save Needed, Help, Software Update</b> , etc.), Internet Explorer cannot open the window and displays the error dialog box. | <ul style="list-style-type: none"> <li>A bug in the Internet Explorer JavaScript interpreter.</li> </ul> | <ol style="list-style-type: none"> <li>Click <b>No</b> on the error dialog box.</li> <li>Log out of the Manager.</li> <li>Close Internet Explorer.</li> <li>Reinstall Internet Explorer.</li> </ol> |

## Command Line Interface errors

These errors may occur while using the menu-based Command Line Interface from a console or Telnet session.

### **ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID.**

| <b>Problem</b>                                                                                | <b>Possible cause</b>                                                                                                                                                                                                                                                          | <b>Solution</b>                                               |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| The system expected a valid 4-byte dotted decimal entry, and the entry wasn't in that format. | <ul style="list-style-type: none"><li>You entered something other than a 4-byte dotted decimal number. You may have omitted a byte position, or entered a number greater than 255 in a byte position.</li><li>You entered 0.0.0.0 instead of an appropriate address.</li></ul> | At the prompt, re-enter a valid 4-byte dotted decimal number. |

### **ERROR:-- Out of Range value entered. Try again.**

| <b>Problem</b>                                                                             | <b>Possible cause</b>                                                                                                                                          | <b>Solution</b>                                            |
|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| The system expected a number within a certain range, and the entry was outside that range. | <ul style="list-style-type: none"><li>You entered a letter instead of a number.</li><li>You entered a number greater than the possible menu numbers.</li></ul> | At the prompt, re-enter a number in the appropriate range. |

### **ERROR:-- The Passwords do not match. Please try again.**

| <b>Problem</b>                                                              | <b>Possible cause</b>                                                                                                                            | <b>Solution</b>                                                                                                                                                                   |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The entry for a password and the entry to verify the password do not match. | <ul style="list-style-type: none"><li>You mistyped an entry.</li><li>You entered either a password or verify entry, but not the other.</li></ul> | At the <i>Verify</i> prompt, re-enter the password. If the original password is incorrect, press <b>Enter</b> and re-enter both the password and the verification at the prompts. |

## LED indicators

LED indicators on the VPN Concentrator and its expansion modules are normally green. The usage gauge LEDs are normally blue. LEDs that are amber or off may indicate an error condition. NA = not applicable; i.e., the LED does not have that state.

Contact Cisco support if any LED indicates an error condition.

## VPN Concentrator LEDs (front)

| LED Indicator (Front)                                      | Green                                                                                                                     | Amber                                                | Off                                                                                      |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>System</b>                                              | Power on. Normal<br><b>Blinking Green</b> (Model 3005 only) = System is in a shutdown (halted) state, ready to power off. | System has crashed and halted. <i>Error.</i>         | (Power off. All other LEDs are off.)                                                     |
| <i>The LEDs below are present only on Models 3015–3080</i> |                                                                                                                           |                                                      |                                                                                          |
| <b>Ethernet Link Status<br/>1 2 3</b>                      | Connected to network and enabled.<br><b>Blinking Green</b> = Connected to network and configured, but disabled.           | NA                                                   | Not connected to network or not enabled.                                                 |
| <b>Expansion Modules<br/>Insertion Status<br/>1 2 3 4</b>  | SEP module or WAN interface module installed in system.                                                                   | NA                                                   | Module not installed in system.                                                          |
| <b>Expansion Modules<br/>Run Status<br/>1 2 3 4</b>        | SEP module or WAN interface module operational.                                                                           | Module failed during operation. <i>Error.</i>        | If installed, module failed diagnostics or encryption code is not running. <i>Error.</i> |
| <b>Fan Status</b>                                          | Operating normally.                                                                                                       | Not running or RPM below normal range. <i>Error.</i> | NA                                                                                       |
| <b>Power Supplies<br/>A B</b>                              | Installed and operating normally.                                                                                         | Voltage(s) outside of normal ranges. <i>Error.</i>   | Not installed.                                                                           |
| <b>CPU Utilization</b>                                     | This statistic selected for usage gauge display.                                                                          | NA                                                   | Not selected.                                                                            |
| <b>Active Sessions</b>                                     | This statistic selected for usage gauge display.                                                                          | NA                                                   | Not selected.                                                                            |
| <b>Throughput</b>                                          | This statistic selected for usage gauge display.                                                                          | NA                                                   | Not selected.                                                                            |

| <b>Usage Gauge LEDs (Front)<br/>(Model 3015–3080 only)</b> | <b>Steady or Intermittent Blue</b> | <b>Blinking Blue</b>                                                  |
|------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------|
| Left to right sequential segments, varying number          | Normal operation.                  | NA                                                                    |
| All 10 segments                                            | NA                                 | VPN Concentrator is in a shutdown (halted) state, ready to power off. |

## VPN Concentrator LEDs (rear)

| <b>LED Indicator (Rear)</b>                                                      | <b>Green</b>                                | <b>Amber</b>              | <b>Off</b>                                     |
|----------------------------------------------------------------------------------|---------------------------------------------|---------------------------|------------------------------------------------|
| <b>Private / Public / External Ethernet Interfaces</b><br>(connected to network) |                                             |                           |                                                |
| <b>Link</b>                                                                      | Carrier detected. Normal.                   | NA                        | No carrier detected. <i>Error.</i>             |
| <b>Tx</b>                                                                        | Transmitting data. Normal. Intermittent on. | NA                        | Not transmitting data. Idle. Intermittent off. |
| <b>Coll</b>                                                                      | NA                                          | Data collisions detected. | No collisions. Normal.                         |
| <b>100</b>                                                                       | Speed set at 100 Mbps.                      | NA                        | Speed set at 10 Mbps.                          |

## SEP (Scalable Encryption Processing) Module LEDs (Model 3015–3080 only)

SEP module LEDs are visible from the rear of the VPN Concentrator.

| <b>SEP Module LED</b> | <b>Green</b>                        | <b>Amber</b>                                  | <b>Off</b>                                                                      |
|-----------------------|-------------------------------------|-----------------------------------------------|---------------------------------------------------------------------------------|
| <b>Power</b>          | Power on. Normal.                   | NA                                            | Power is not reaching the module. It may not be seated correctly. <i>Error.</i> |
| <b>Status</b>         | Encryption code is running. Normal. | Module failed during operation. <i>Error.</i> | Module failed diagnostics or encryption code is not running. <i>Error.</i>      |

## WAN Interface Module LEDs

WAN module LEDs are visible from the rear of the VPN Concentrator.

| WAN Module LED | On                                                        | Blinking                                 | Off                                                                                |
|----------------|-----------------------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------|
| <b>Power</b>   | Normal operation.                                         | NA                                       | Power is not reaching the module. It may not be seated correctly.<br><i>Error.</i> |
| <b>Status</b>  | Module has passed diagnostics and is operational. Normal. | Module failed diagnostics. <i>Error.</i> | Module has failed.<br><i>Error.</i>                                                |

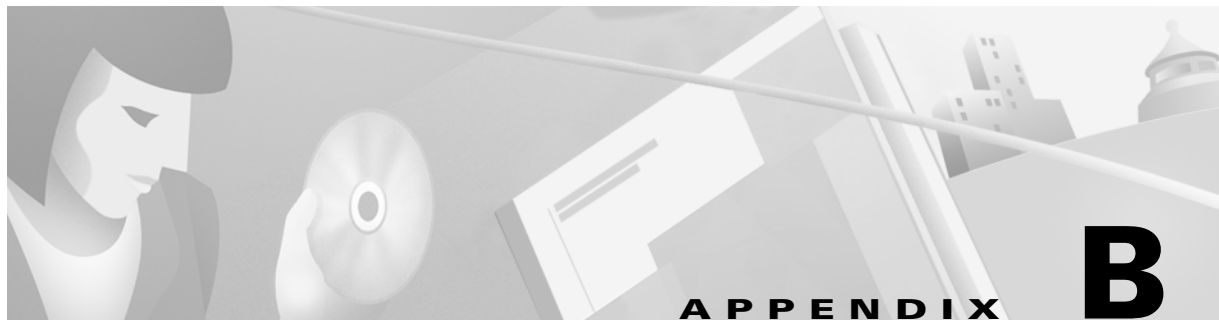
This table shows all possible combinations for the LEDs on each WAN Port.

| <b>WAN Port LEDs</b>                         |                             |                                |                         |                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------|-----------------------------|--------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alrm</b><br>Alarm                         | <b>CD</b><br>Carrier Detect | <b>Sync</b><br>Synchronization | <b>LpBk</b><br>Loopback | <b>Condition</b>                                                                                                                                                                                                                                                                                                                                                         |
| Off                                          | <b>On</b>                   | <b>On</b>                      | Off                     | Normal operation.<br>Carrier detected,<br>line in synchronization.                                                                                                                                                                                                                                                                                                       |
| Off                                          | Off                         | Off                            | <b>On</b>               | Line is in loopback mode. This mode occurs, for example, when you install the line and the carrier is testing the signal.<br><br>You can also set loopback mode by pressing the <b>LpBk</b> switch. <b>LpBk</b> is a recessed momentary-contact switch that sets loopback mode in this sequence:<br><br>Port A on<br>Port B on<br>Ports A and B on<br>Ports A and B off. |
| <b>All four Port LEDs blinking in unison</b> |                             |                                |                         | Port configured but not enabled.                                                                                                                                                                                                                                                                                                                                         |
| <b>T1/E1 Line Error Condition</b>            |                             |                                |                         |                                                                                                                                                                                                                                                                                                                                                                          |
| <b>On</b>                                    | Off                         | Off                            | Off                     | <b>“Red”</b> = Complete loss of signal. Possible causes: out-of-frame errors, mismatched framing format (e.g., one side using SF and the other using ESF), or disconnected line.                                                                                                                                                                                         |
| <b>On</b>                                    | Off                         | Off                            | <b>On</b>               | <b>“Red”</b> in loopback mode.                                                                                                                                                                                                                                                                                                                                           |
| <b>On</b>                                    | <b>On</b>                   | <b>On</b>                      | Off                     | <b>“Yellow”</b> = Problem in transmit path; i.e., the remote connection has detected a problem on this line.                                                                                                                                                                                                                                                             |
| <b>On</b>                                    | <b>On</b>                   | <b>On</b>                      | <b>On</b>               | <b>“Yellow”</b> in loopback mode.                                                                                                                                                                                                                                                                                                                                        |
| <b>On</b>                                    | <b>On</b>                   | Off                            | Off                     | <b>“Blue”</b> = Problem in receive path; i.e., the line has lost synchronization with the remote connection.                                                                                                                                                                                                                                                             |
| <b>On</b>                                    | <b>On</b>                   | Off                            | <b>On</b>               | <b>“Blue”</b> in loopback mode.                                                                                                                                                                                                                                                                                                                                          |

End of Appendix







## Copyrights, licenses, and notices

---

### Software License Agreement of Cisco Systems, Inc.

CISCO SYSTEMS, INC. IS WILLING TO LICENSE TO YOU THE SOFTWARE CONTAINED IN THE ACCOMPANYING CISCO PRODUCT ONLY IF YOU ACCEPT ALL OF THE TERMS AND CONDITIONS IN THIS LICENSE AGREEMENT. PLEASE READ THIS AGREEMENT CAREFULLY BEFORE YOU OPEN THE PACKAGE BECAUSE, BY OPENING THE SEALED PACKAGE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CISCO SYSTEMS WILL NOT LICENSE THIS SOFTWARE TO YOU. IN THAT CASE YOU SHOULD RETURN THE PRODUCT PROMPTLY, INCLUDING THE PACKAGING, THE UNOPENED PACKAGE, ALL ACCOMPANYING HARDWARE, AND ALL WRITTEN MATERIALS, TO THE PLACE OF PURCHASE FOR A FULL REFUND.

#### Ownership of the Software

1. The software contained in the accompanying Cisco product (“the Software”) and any accompanying written materials are owned or licensed by Cisco Systems and are protected by United States copyright laws, laws of other nations, and/or international treaties.

#### Grant of License

2. Cisco Systems hereby grants to you the right to use the Software with the Cisco VPN 3000 Concentrator product. To this end, the Software contains both operator software for use by the network administrator and client software for use by clients at remote network nodes. You may transfer the client software, or portions thereof, only to prospective nodes on the network, and to no one else. You may not transfer the operator software.

#### Restrictions on Use and Transfer

3. You may not otherwise copy the Software, except that you may make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single disk provided you keep the disk solely for backup or archival purposes. You may not copy the written materials and you may not use the backup or archival copy of the Software except in conjunction with the accompanying Cisco product.

4. You may permanently transfer the Software and accompanying written materials (including the most recent update and all prior versions) only in conjunction with a transfer of the entire Cisco product, and only if you retain no copies and the transferee agrees to be bound by the terms of this Agreement. Any transfer terminates your license. You may not rent or lease the Software or otherwise transfer or assign the right to use the Software, except as stated in this paragraph.
5. You may not export the Software, even as part of the Cisco product, to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software, even as part of the Cisco product, in violation of any export control laws of the United States or any other country.
6. You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or accompanying documentation or any copy thereof, in whole or in part.
7. The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy, or return to Cisco Systems, the Software and accompanying documentation and all copies thereof. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.
8. You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 and 3 hereof.
9. You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.
10. Any notice, demand, or request with respect to this Agreement shall be in writing and shall be effective only if it is delivered by hand or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to Cisco Systems, whose address is set forth below. Such communications shall be effective when they are received by Cisco Systems.

## **Limited Warranty**

11. Cisco Systems warrants that the Software will perform substantially in accordance with the accompanying written materials for a period of 90 days from the date of your receipt of the Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.
12. CISCO SYSTEMS DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, WITH RESPECT TO THE SOFTWARE, THE ACCOMPANYING WRITTEN MATERIALS, AND THE ACCOMPANYING HARDWARE. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.
13. CISCO SYSTEMS' ENTIRE LIABILITY AND YOUR EXCLUSIVE REMEDY SHALL BE, AT CISCO SYSTEMS' CHOICE, EITHER (A) RETURN OF THE PRICE PAID OR (B) REPLACEMENT OF THE SOFTWARE THAT DOES NOT MEET CISCO SYSTEMS' LIMITED WARRANTY AND WHICH IS RETURNED TO CISCO SYSTEMS TOGETHER WITH A COPY OF YOUR RECEIPT. Any replacement Software will be warranted for the remainder of the original warranty period or 30 days, whichever is longer. These remedies are not available outside the United States of America.
14. This Limited Warranty is void if failure of the Software has resulted from modification, accident, abuse, or misapplication.
15. IN NO EVENT WILL CISCO SYSTEMS BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY LOSS OF PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE SOFTWARE. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

16. This Agreement is governed by the laws of the State of Massachusetts.

17. If you have any questions concerning this Agreement or wish to contact Cisco Systems for any reason, please call (508) 541-7300, or write to

Cisco Systems, Inc.

124 Grove Street, Suite 205

Franklin, Massachusetts 02038.

18. U.S. Government Restricted Rights. The Software and accompanying documentation are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph (c)(1) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1)(ii) and (2) of Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Supplier is Cisco Systems, Inc., 124 Grove Street, Suite 205, Franklin, Massachusetts 02038.

19. This Agreement constitutes the entire agreement between Cisco Systems and the licensee. There are no understandings, agreements, representations, or warranties, expressed or implied, not specified herein regarding this Agreement or the Software licensed hereunder. Only the terms and conditions contained in this Agreement shall govern the transaction contemplated hereunder, notwithstanding any additional, different, or conflicting terms which may be contained in any purchase order or other documents pertaining to the subject transaction.

## Other licenses

The VPN 3000 Concentrator Series contains and uses software from other firms, under license. Relevant copyright and license notices follow.

## BSD software

Copyright © 1990, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### DHCP client

Copyright © 1995, 1996, 1997 The Internet Software Consortium.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of The Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INTERNET SOFTWARE CONSORTIUM OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### DNS Resolver (client)

DNS Resolver / BSD / DEC / Internet Software Consortium

Copyright © 1988, 1993

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright © 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED “AS IS” AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission.

To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product.

THE SOFTWARE IS PROVIDED “AS IS”, AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

## IPSec

COPYRIGHT 1.1a (NRL) 17 August 1995

### COPYRIGHT NOTICE

All of the documentation and software included in this software distribution from the US Naval Research Laboratory (NRL) are copyrighted by their respective developers.

This software and documentation were developed at NRL by various people. Those developers have each copyrighted the portions that they developed at NRL and have assigned All Rights for those portions to NRL. Outside the USA, NRL also has copyright on the software developed at NRL. The affected files all contain specific copyright notices and those notices must be retained in any derived work.

NRL LICENSE

NRL grants permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation created at NRL provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed at the Information Technology Division, US Naval Research Laboratory.

4. Neither the name of the NRL nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THE SOFTWARE PROVIDED BY NRL IS PROVIDED BY NRL AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NRL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the US Naval Research Laboratory (NRL).

## LDAP

Copyright © 1992-1996 Regents of the University of Michigan.  
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

## Outline style table of contents in JavaScript

OUTLINE STYLE TABLE OF CONTENTS in JAVASCRIPT  
Version 3.0  
by Danny Goodman (dannyg@dannyg.com)  
Analyzed and described at length in  
"JavaScript Bible"  
by Danny Goodman  
(IDG Books ISBN 0-7645-3022-4)

This program is Copyright 1996, 1997, 1998 by Danny Goodman. You may adapt this outline for your Web pages, provided these opening credit lines (down to the lower dividing line) are in your outline HTML document. You may not reprint or redistribute this code without permission from the author.

## RSA software



Copyright © 1995-1998 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

BSAFE is a trademark of RSA Data Security, Inc.

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.

## SecureID

SecureID is a product of RSA Security Inc., Bedford, MA. (formerly Security Dynamics Technologies, Inc.)

Use of SDTI's Trade Name and Trademarks

- (a) Any advertising or promotional literature or announcement to the press by the Partner regarding its relationship with SDTI, or otherwise utilizing SDTI's name or trademarks must be approved by SDTI in writing in advance, which approval will not be unreasonably withheld or delayed.
- (b) The Partner shall include and shall not alter, obscure or remove any SDTI name or any other trademark or trade name used by SDTI or any markings, colors or other insignia which are contained on or in or fixed to the Software (collectively, "Proprietary Marks"). Partner agrees to include SDTI's copyright notice in its help screen as it pertains to the SDTI Translation.

## Server SNMP

Copyright 1998 by Carnegie Mellon University  
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Client SNMP

Copyright © 1996, 1997 by Westhawk Ltd.

([www.westhawk.co.uk](http://www.westhawk.co.uk))

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

author [tpanton@ibm.net](mailto:tpanton@ibm.net) (Tim Panton)

## SSL Plus

Certicom, the Certicom logo, SSL Plus, and Security Builder are trademarks of Certicom Corp. Copyright © 1997-1999 Certicom Corp. Portions are Copyright © 1997-1998, Consensus Development Corporation, a wholly owned subsidiary of Certicom Corp. All rights reserved.

Contains an implementation of NR signatures, licensed under U.S. patent 5,600,725. Protected by U.S. patents 5,787,028; 4,745,568; 5,761,305. Patents pending.

## TCP compression / uncompression

Routines to compress and uncompress TCP packets (for transmission over low speed serial lines).

Copyright © 1989 Regents of the University of California.  
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Van Jacobson (van@helios.ee.lbl.gov), Dec 31, 1989:  
- Initial distribution.

Modified for KA9Q Internet Software Package by Katie Stevens (dkstevens@ucdavis.edu)  
University of California, Davis  
Computing Services

|            |                                       |                                               |
|------------|---------------------------------------|-----------------------------------------------|
| - 01-31-90 |                                       | initial adaptation (from 1.19)                |
| PPP.05     | 02-15-90 [ks]                         |                                               |
| PPP.08     | 05-02-90 [ks]                         | use PPP protocol field to signal compression  |
| PPP.15     | 09-90 [ks]                            | improve mbuf handling                         |
| PPP.16     | 11-02 [karn]                          | substantially rewritten to use NOS facilities |
| - Feb 1991 | Bill_Simpson@um.cc.umich.edu          |                                               |
|            | variable number of conversation slots |                                               |
|            | allow zero or one slots               |                                               |
|            | separate routines                     |                                               |
|            | status display                        |                                               |

## Telnet server

Copyright phase2 networks 1996  
All rights reserved

SID: 1.1

Revision History:

1.1 97/06/23 21:17:43 root



# Regulatory Agency Notices

## U.S. Federal Communications Commission (FCC) Compliance Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

## E.U. EN 55022 Notice

**Warning:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## Voluntary Control Council for Interference by Information Technology Equipment (VCCI) Statement

(1) Class A ITE (Information Technology Equipment) shall be identified with a label containing the following statement at a conspicuous location on the equipment and in the instruction manual.

この装置は、第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI- A

(Translation)

Warning

This is a Class 1 product.

In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. VCCI-A

Note 1. \*VCCI-A: Equipment satisfying the recommended values for Class A ITE.

## WAN Module Customer Instructions: FCC Requirements

### Notice to Users of T1 Service

The following instructions are provided to ensure compliance with the Federal Communications Commission (FCC) Rules, Part 68.

- (1) -----
- (2) Before connecting your unit, you must inform the telephone company of the following information:

| Port ID   | REN/SOC | FIC       | USOC  |
|-----------|---------|-----------|-------|
| Port 0, 1 | 6.0N    | 04DU9-1SN | RJ48C |

- (3) If the unit appears to be malfunctioning, it should be disconnected from the telephone lines until you learn if your equipment or the telephone line is the source of the trouble. If your equipment needs repair, it should not be reconnected until it is repaired.
- (4) If the telephone company finds that this equipment is exceeding tolerable parameters, the telephone company can temporarily disconnect service, although they will attempt to give you advance notice if possible.
- (5) Under the FCC Rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or out of warranty.
- (6) If the telephone company alters their equipment in a manner that will affect use of this device, they must give you advance warning so as to give you the opportunity for uninterrupted service. You will be advised of your right to file a complaint with the FCC.
- (7) The attached Affidavit (Appendix A) must be completed by the installer.
- (8) **Service Requirements:** In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be facilitated through our office at:

**Cisco Systems, Inc.**  
**170 West Tasman Drive**  
**San Jose, CA 95134-1706**

## Notice to Users of Certified Component Devices

The following instructions are provided to ensure compliance with the Federal Communications Commission (FCC) Rules, Part 68.

This equipment is certified with the FCC under Part 68 as a component device for use with the following Cisco Systems host routers:

In order for the FCC certification of this product to be retained, all other products used in conjunction with this product must also be FCC Part 68 certified for use with these hosts. If any of these components are not certified, then you are required to obtain FCC Part 68 certification of the assembled equipment prior to connection to the telephone network. Part 68 certification requires that you maintain this approval and as such are responsible for the following:

- Any component added to your equipment, whether it bears component certification or not, will require a Part 68 compliance evaluation. You may need to test and make a modification filing to the FCC before that new component can be used;
- Any modification/update made by a manufacturer to any certified component within your equipment, will require a Part 68 compliance evaluation. You may need to test and make a modification filing to the FCC before that modified component can be used;
- If you continue to produce this compound you are required to comply with the FCC's Continuing Compliance requirements. Therefore is it recommended that only FCC Part 68 certified devices bearing the 'CN' or 'CE' equipment code as part of the FCC certification number, be used (NOTE: The host equipment used in conjunction with this product may bear an FCC Certification number with other than the 'CN' or 'CE' equipment code). In determining if your particular component device is appropriately approved, look for the FCC certification number on all components and ensure that the classification code '-CN-' or '-CE-' is part of that number. Refer to the FCC Certification number on this product as an example.

- If the telephone company requests that you supply the FCC Certification number and REN of the device you are connecting, please supply the FCC Certification numbers from all component and host devices that have a direct PSTN connection (i.e. have a REN stated on the label) and the highest REN.
- If at any time the ownership of this component device is transferred to someone else (whether independently or as part of a system), supply this manual to the new owner.

## Affidavit (Appendix A)

### AFFIDAVIT FOR CONNECTION OF CUSTOMER PREMISES EQUIPMENT TO 1.544 MBPS AND/OR SUBRATE DIGITAL SERVICES

For the work to be performed in the certified territory of \_\_\_\_\_ (Telco Name)

State of \_\_\_\_\_

County of \_\_\_\_\_

I, \_\_\_\_\_ (name), \_\_\_\_\_ (business address)  
 \_\_\_\_\_ (telephone number) being duly sworn, state:

I have responsibility for the operation and maintenance of the terminal equipment to be connected to 1.544 Mbps and/or \_\_\_\_\_ subrate digital services. The terminal equipment to be connected complies with Part 68 of the FCC rules except for the encoded analog content and billing protection specifications. With respect to encoded analog content and billing protection:

- I attest that all operations associated with the establishment, maintenance and adjustment of the digital CPE with respect to analog content and encoded billing protection information continuously complies with Part 68 of the FCC Rules and Regulations.
- The digital CPE does not transmit digital signals containing encoded analog content or billing information which is intended to be decoded within the telecommunication network.
- The encoded analog content and billing protection is factory set and is not under the control of the customer.

I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions be successfully having completed one of the following: (Check appropriate blocks).

- A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or
- An independent training course (e.g., trade school or technical institution) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or
- In lieu of the preceding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with \_\_\_\_\_ (circle one) above.

I agree to provide \_\_\_\_\_ (Telco's name) with proper documentation to demonstrate compliance with the information as provided in the preceding paragraph, if so requested.

\_\_\_\_\_ Signature

\_\_\_\_\_ Title

\_\_\_\_\_ Date

Subscribed and sworn to before me

This      day of              , 20\_\_\_\_

\_\_\_\_\_  
 Notary Public

My commission expires:

## **WAN Module: CS03 Canadian Requirements— Equipment Attachment Limitations**

**NOTICE:** The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunications Company. The equipment must also be installed using an acceptable method of connection. In some cases, the companies inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorised Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

**Caution:** Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Industry Canada CS-03 Application, Rev.1  
Model No.: CVPN 3000-2T1

**End of Appendix**



## Numerics

100 LED (Ethernet) A-11

## A

about this manual xxxvii

access control list, administration 14-26

add 14-27

modify 14-27

access hours, configuring 13-2

add 13-4

modify 13-4

access rights, configuring for administrators 14-24

access rights section, administration 14-21

access settings, general, for administrators 14-28

accessing the CLI 16-1

accounting record attributes, RADIUS 5-12

accounting servers

configuring 5-11

add 5-13

modify 5-13

accounting statistics 15-68

Active Sessions LED A-10

add

access control list, administration 14-27

access hours 13-4

accounting server 5-13

address pool 6-4

authentication server 5-3

DHCP server 5-18

email recipient of events 10-22

event class 10-11

filter rule (traffic management) 13-12

filter (traffic management) 13-31

group (user management) 12-18

IKE proposal 7-22

IPSec LAN-to-LAN connection 7-10

NAT rule 13-42

network list 13-7

NTP host 5-21

OSPF area 8-9

security association to rule on filter 13-36

security association (traffic management) 13-22

SMTP server for events 10-20

SNMP community 9-10

SNMP event destination 10-15

static route for IP routing 8-3

syslog server to receive events 10-17

user on internal server (user management) 12-34

address management, configuring 6-1

address pools

configuring 6-3

add 6-4

modify 6-4

statistics 15-76

admin password, default 14-22

administering the VPN Concentrator 14-1

administration, access control list 14-26

add 14-27

modify 14-27

administration section of Manager 14-1

Administration (tab on Manager screen) 1-21

administrators

access rights 14-21, 14-24

access settings, general 14-28

configuring 14-21

default passwords 14-22

default rights, table 14-24

file rights 14-25

locking configuration 14-7

modify properties 14-23

parameters in nonvolatile memory 14-22

predefined 14-21

session idle timeout 14-28

alarm thresholds, power, configuring 3-5

Alrm LED (WAN) A-13

ARP table 15-94

assign rules to filter (traffic management) 13-34

assignment of IP addresses, configuring 6-2

authentication parameters, order of checking 12-1

authentication servers

configuring 5-2

add 5-3

internal 5-8

modify 5-3

NT Domain 5-5

RADIUS 5-4

SecurID 5-6

testing 5-9

authentication statistics 15-66

autodiscovery, network 7-8, 7-14  
automatic switchover (redundancy) 8-12

**B**

back panel display (monitoring) 15-10  
Bad IP Address (error) A-8  
base group, configuring (user management) 12-3  
bibliography xxxix  
bootcode  
    filename 15-10  
    version 15-10  
browser  
    Back or Forward button displays incorrect screen or incorrect data A-2  
    clear cache after software update 14-16  
    installing SSL certificate 1-3  
    navigation toolbar, don't use with Manager 1-2  
    Refresh / Reload button logs out the Manager A-2  
    requirements 1-1  
built-in servers, configuring  
    *See* management protocols 9-1

**C**

CD LED (WAN) A-13  
Certificate Authority  
    *See* digital certificates  
certificate management 14-34  
change security association on rule 13-37  
Cisco Connection Online Web page 1-20  
Cisco, contacting xli  
Cisco Systems (logo) 1-22  
Cisco VPN 3000 Client  
    IPSec attributes 7-7, 13-20  
    IPSec support 12-6, 12-23, 12-38  
    supports Mode Configuration 12-9, 12-27  
clear event log 15-7  
CLI  
    access rights 16-7  
    accessing 16-1  
        via console 16-1  
        via Telnet 16-2  
    entering values 16-3  
    errors A-8  
    help command 16-6  
    main menu 16-2  
    menu reference 16-8  
    menus, navigating 16-5  
    saving configuration file 16-7  
    specifying configured items 16-4  
    starting 16-2  
    stopping 16-7  
    using 16-1, 16-3  
    using Back and Home 16-6  
    using shortcut numbers to navigate 16-5

closed or collapsed (icon) 1-22  
Coll LED (Ethernet) A-11  
Command Line Interface  
    *See* CLI  
configuration files  
    changes with software update 14-14  
    handling at reboot or shutdown 14-18  
    saving 1-21  
        CLI 16-7  
    swap 14-32  
    useful for troubleshooting A-2  
configuration section of Manager 2-1  
Configuration (tab on Manager screen) 1-21  
configuring VPN Concentrator with CLI 16-1  
connecting to VPN Concentrator  
    using HTTP 1-3  
    using HTTPS 1-17  
console, accessing CLI via 16-1  
contacting Cisco with questions xli  
conventions  
    documentation xxxix  
    typographic xxxix  
cookies, requirements 1-2  
copy  
    filter rule (traffic management) 13-12  
    filter (traffic management) 13-31  
    IKE proposal 7-22  
    network list 13-7  
copyrights and licenses B-1  
CPU Utilization LED A-10  
crash, system, saves log file 10-6, A-1  
CRSHDUMP . TXT file A-1

**D**

data  
    formats xli  
    top ten sessions sorted by 15-41  
date and time, configuring 11-3  
Daylight-Saving Time, enabling 11-3  
default  
    administrator passwords 14-22  
    administrator rights, table 14-24  
    event handling, configuring 10-6  
    filter rules  
        table 13-10  
        using 13-9  
    filters  
        table 13-30  
        using 13-29  
    gateways, configuring for IP routing 8-5  
    IKE proposals, table 7-20  
    security associations, table 13-21  
    tunnel gateway, configuring 8-5

- delete
    - digital certificate 14-49
    - filter rule (traffic management) 13-19
    - group (user management) 12-17
    - internal authentication server 5-8
    - security association (traffic management) 13-28
    - user on internal server (user management) 12-34
  - DHCP
    - functions within the VPN Concentrator, configuring 8-10
    - servers, configuring 5-16
      - add 5-18
      - modify 5-18
    - statistics 15-75
  - digital certificates
    - Certificate Revocation List (CRL) checking 14-46
    - CRL distribution point 14-47
    - deleting 14-42, 14-49
    - display all 14-42
    - enrolling with a Certificate Authority 14-40
    - enrollment request 14-36
    - generating SSL 14-43
    - identity 14-34
    - in IPSec LAN-to-LAN 7-13
    - installing 14-36, 14-40
    - managing 14-34
    - PKCS-10 request 14-39
    - root 14-34
    - SSL 14-35
    - viewing details 14-44
    - X.509 14-35
  - display settings 1-2
  - DNS
    - configuring for group 12-22
    - servers, configuring 5-14
    - statistics 15-65
  - documentation
    - additional xxxviii
    - Cisco Web page 1-20
    - conventions xxxix
  - dual T1/E1 WAN
    - interface, configuring 3-16
    - system status 15-14
  - duration, top ten sessions sorted by 15-43
- E**
- email recipients of events, configuring 10-20
    - add 10-22
    - modify 10-22
  - encryption algorithms used by sessions (monitoring) 15-39
  - enrolling with a Certificate Authority 14-40
  - entering values with CLI 16-3
  - error
    - an error has occurred ... A-4
    - bad IP address A-8
    - insufficient authorization A-6
    - invalid login A-3
    - JavaScript A-5
    - no such interface supported (IE) A-7
    - not allowed A-6
    - not found A-7
    - old browser A-5
    - out of range value A-8
    - passwords do not match A-8
    - session timeout A-3
  - errors
    - and troubleshooting A-1
    - CLI A-8
    - VPN Concentrator Manager A-2
  - Ethernet interfaces
    - See also* interfaces
  - Ethernet Link Status LEDs A-10
  - Ethernet MIB-II statistics 15-96
  - event classes
    - configuring for special handling 10-10
      - add 10-11
      - modify 10-11
    - table 10-1
  - event log 10-5
    - capacity 10-5, 15-4
    - clear (erase) 15-7
    - deleting from flash memory 10-6
    - download to PC 15-6
    - file size 10-6
    - format of 15-7
    - get 15-6
    - monitoring 15-4
    - save 10-6, 15-6
    - save on VPN Concentrator 15-6
    - saved at system reboot 10-6, A-1
    - saved if system crashes 10-6, A-1
    - saving in flash memory 10-6
    - saving via FTP 10-7, 10-9
    - stored in nonvolatile memory 15-4
    - view 15-4, 15-6
  - event severity levels, table 10-4
  - event trap destinations, configuring 10-14
  - events
    - configuring default handling 10-6
    - configuring handling 10-5
    - configuring special handling 10-10
    - section of Manager 10-1
    - statistics 15-62
  - exiting
    - from CLI 16-7
    - the Manager (logout) 1-21

Expansion Modules Insertion Status LEDs A-10  
Expansion Modules Run Status LEDs A-10  
Extended Authentication, IPSec 12-9, 12-26

## **F**

Fan Status LED A-10  
fans, cooling (monitoring) 15-11  
file access rights, administrators' 14-25  
file management on VPN Concentrator 14-29, 14-30  
file transfer, TFTP 14-32  
filenames, format xl  
filter 13-1

- add security association to rule on 13-36
- add (traffic management) 13-31
- assign rules to (traffic management) 13-34
- configuring on base group 12-5
- configuring on group 12-22
- configuring on interface
  - Ethernet 3-9
  - WAN 3-18
- configuring on user 12-38
- configuring (traffic management) 13-28
- copy (traffic management) 13-31
- default
  - table 13-30
  - using 13-29
- modify (traffic management) 13-31

filter rules 13-1

- add (traffic management) 13-12
- configuring 13-9
- copy (traffic management) 13-12
- default
  - table 13-10
  - using 13-9
- delete (traffic management) 13-19
- modify (traffic management) 13-12

filtering statistics 15-69  
flash memory

- corrupting 14-14, 14-17
- file transfer via TFTP 14-32
- managing files in 14-29, 14-30
- rights to files in 14-25
- saving log files in 10-6
- size of 14-30
- space used 14-30

formats

- data xl
- filenames xl
- hostnames xl
- IP addresses xl
- MAC addresses xl
- port numbers xl
- subnet masks xl

text strings xl  
wildcard masks xl  
fractional T1/E1 interface 3-16, 3-24  
front panel display (monitoring) 15-10  
FTP

- configuring internal server 9-2
- using to save log files 10-7, 10-9

Funk Steel-Belted RADIUS 5-2, 12-1

## **G**

gateways, default 8-5  
general parameters, configuring 11-1  
generating SSL server certificate 14-43  
get event log 15-6  
groups, configuring, user management 12-16

- add 12-18
- delete 12-17
- modify external 12-32
- modify internal 12-18

## **H**

halt system 14-17  
help, CLI 16-6  
Help (tab on Manager screen) 1-20  
hostnames, format xl  
HTTP

- configuring internal server 9-3
- statistics 15-61
- using with Manager 1-3

HTTPS

- configuring internal server 9-3
- connecting using 1-17
- login screen 1-17

## **I**

ICMP MIB-II statistics 15-92  
icon

- Cisco Systems logo 1-22
- closed or collapsed 1-22
- open or expanded 1-22
- Refresh 1-22
- Save 1-21
- Save Needed 1-21

identity certificates 14-34  
idle timeout for administrator sessions 14-28  
IKE proposals

- active 7-21
- configuring 7-19
  - add 7-22
  - copy 7-22
  - modify 7-22



- IKE proposals (continued)
    - default, table 7-20
    - in IPSec LAN-to-LAN 7-14
    - in security association 13-19
    - inactive 7-21
  - IKE security association
    - See* security associations
  - image, software
    - filenames 14-15
    - update 14-14
  - indicators, LED A-9
  - Install SSL Certificate (screen) 1-4
  - installing digital certificates 14-36, 14-40
  - installing SSL certificate
    - with Internet Explorer 1-4
    - with Netscape 1-10
  - interfaces
    - configuring 3-2
    - dual T1/E1 (WAN) 3-16
    - Ethernet, configuring 3-7
      - OSPF 3-11
      - RIP 3-10
      - speed 3-9
      - transmission mode 3-9
    - Ethernet status and statistics 15-12
    - filter
      - Ethernet 3-9
      - WAN 3-18
    - fractional T1/E1 3-16
    - MIB-II statistics 15-78
    - public 3-8, 3-17, 7-10, 13-42
    - section of Manager 3-1
    - status 3-4, 3-14
    - WAN, configuring 3-14, 3-16
      - filter 3-18
      - MP 3-25
      - OSPF 3-20
      - RIP 3-18
      - select T1 or E1 3-15
      - T1/E1 parameters 3-23
      - timeslots 3-24
    - WAN status and statistics 15-14
  - internal authentication server
    - configuring 5-8
    - deleting 5-8
  - Internet Explorer, requirements 1-1
  - Invalid Login or Session Timeout (error) A-3
  - IP addresses
    - configuring assignment of 6-2
    - format xl
  - IP MIB-II statistics 15-82
  - IP routing
    - configuring 8-2
    - section of Manager 8-1
  - IPSec
    - Cisco VPN 3000 Client 7-7, 12-6, 12-23, 12-38, 13-20
    - configuring 7-7
      - base group 12-6, 12-7
      - group (internal) 12-23, 12-24
      - user (internal server) 12-38, 12-39
    - discussion 7-7
    - Mode Configuration 12-9, 12-26
    - rules 13-5
    - security associations
      - See* security associations
    - statistics 15-55
    - XAuth 12-9, 12-26
  - IPSec LAN-to-LAN
    - automatic parameters 7-11, 7-18, 13-14
    - configuring 7-8
      - add connection 7-10
      - modify connection 7-10
      - no public interfaces screen 7-10
      - on WAN interface 7-8
      - parameters for redundant systems 8-12
    - Done (screen) 7-18
    - rules that apply IPSec 13-14
    - using network lists 7-12, 7-14, 7-16
  - IPSec over UDP, discussion 12-11
  - IPSec through NAT
    - configuring
      - base group 12-11
      - group 12-28
    - discussion 12-11
- ## J
- JavaScript (error) A-5
  - JavaScript, requirements 1-1
- ## L
- L2TP
    - configuring
      - base group 12-6, 12-12
      - group (internal) 12-23, 12-28
      - user (internal server) 12-38, 12-41
    - configuring system-wide parameters 7-5
    - statistics 15-51
  - L2TP over IPSec
    - configuring
      - base group 12-7
      - group (internal) 12-23
      - user (internal server) 12-39
    - default security association to use 12-8, 12-25, 12-40
    - don't use Mode Configuration 12-9, 12-26
    - IKE proposal required 7-21
    - no IPSec user authentication 12-9, 12-26
    - parameters differ from IPSec 12-2
    - Windows 2000 client support 7-1, 12-7, 12-23, 12-39

## LAN-to-LAN

*See* IPsec LAN-to-LAN

## LED indicators

- 100 (Ethernet) A-11
- Active Sessions A-10
- Alrm (WAN) A-13
- CD (WAN) A-13
- Coll (Ethernet) A-11
- CPU Utilization A-10
- Ethernet Link Status A-10
- Expansion Modules Insertion Status A-10
- Expansion Modules Run Status A-10
- Fan Status A-10
- Link (Ethernet) A-11
- LpBk (WAN) A-13
- Power (SEP) A-11
- Power Supplies (front panel) A-10
- Power (WAN) A-12
- status, front panel 15-25
- Status (SEP) A-11
- Status (WAN) A-12
- Sync (WAN) A-13
- System A-10
  - table A-9
- Throughput A-10
- Tx (Ethernet) A-11
- usage gauge (blue) A-11
- WAN card A-12

left frame (table of contents) in Manager window 1-22

licenses and copyrights B-1

Link LED (Ethernet) A-11

locked configuration 14-7

log files

*See* event log

logging in the VPN Concentrator Manager 1-18

logging out all sessions 14-4

login

name

current (Manager) 1-21

factory default (Manager) 1-18

password, factory default (Manager) 1-18

screen 1-3

HTTPS 1-17

Internet Explorer 1-8

Netscape 1-14

Logout (tab on Manager screen) 1-21

loopback mode, setting on WAN card A-13

LpBk LED (WAN) A-13

**M**

MAC addresses, format xl

main frame (Manager screen) in Manager window 1-22

main menu, CLI 16-2

Main (tab on Manager screen) 1-20

management protocols, configuring 9-1

Manager table of contents 1-24

Manager toolbar, in Manager window 1-20

Manager window

Cisco Systems logo 1-22

left frame (table of contents) 1-22

main frame 1-22

mouse pointer and tips 1-20

status bar 1-19

title bar 1-19

top frame (Manager toolbar) 1-20

managing VPN Concentrator with CLI 16-1

memory, SDRAM 15-10

menus, CLI, navigating 16-5

MIB-II

statistics 15-77

system object 11-2

Mode Configuration, IPsec 12-9, 12-26

and split tunneling 12-9, 12-26

Cisco VPN 3000 Client supports 12-9, 12-27

model number, system 15-10

modify

access control list, administration 14-27

access hours 13-4

accounting server 5-13

address pool 6-4

authentication server 5-3

DHCP server 5-18

email recipient of events 10-22

event class 10-11

filter rule (traffic management) 13-12

filter (traffic management) 13-31

group (external) (user management) 12-32

group (internal) (user management) 12-18

IKE proposal 7-22

IPsec LAN-to-LAN connection 7-10

NAT rule 13-42

network list 13-7

NTP host 5-21

OSPF area 8-9

properties of administrators 14-23

security association (traffic management) 13-22

SMTP server for events 10-20

SNMP community 9-10

SNMP event trap destination 10-15

static route, for IP routing 8-3

syslog server to receive events 10-17

user on internal server (user management) 12-34

monitor / display settings 1-2

monitoring

screens, automatic refresh 14-20

section of Manager 15-1

Monitoring (tab on Manager screen) 1-21

mouse pointer and tips in Manager window 1-20  
 multilink PPP (MP), configuring 3-25

## N

### NAT

configuring 13-39  
 enable 13-40  
 many-to-one translation 13-39  
 no public interfaces screen 13-42

### NAT rules, configuring 13-40

add 13-42  
 modify 13-42

### navigating

CLI menus 16-5  
 the VPN Concentrator Manager 1-24

### Netscape Navigator, requirements 1-1

network autodiscovery 7-8, 7-14

### network lists 13-1

and split tunneling 12-10  
 configuring 13-6  
 add 13-7  
 automatic generation 13-8  
 copy 13-7  
 modify 13-7

IPSec LAN-to-LAN 7-12, 7-14, 7-16

### network time, configuring

*See* NTP 5-18

### No Public Interfaces screen

IPSec LAN-to-LAN 7-10  
 NAT 13-42

### No such interface supported (error) A-7

### nonvolatile memory 14-22

event log stored in 15-4

### Not Allowed (error) A-6

### Not Found (error) A-7

### notices, regulatory agency B-9

### NT Domain, configuring authentication server 5-5

### NTP, configuring 5-18

hosts (servers) 5-20  
 add 5-21  
 modify 5-21  
 synchronization 5-19

## O

### old browser (error) A-5

### open or expanded (icon) 1-22

### organization of the VPN Concentrator Manager 1-23

### OSPF 3-1, 3-2

configuring  
 on Ethernet interface 3-11  
 on WAN interface 3-20  
 system-wide parameters 8-6

MIB-II statistics 15-87

### OSPF areas, configuring 8-8

add 8-9  
 modify 8-9

### Out of Range value (error) A-8

## P

### password

default administrator 14-22  
 factory default (Manager) 1-18

### Passwords do not match (error) A-8

### ping a host 14-19

### PKCS-10 enrollment request 14-39

### policy management

configuring 13-2  
 section of Manager 13-1

### port numbers, format xl

### ports, WAN 3-16

### Power LED (SEP) A-11

### Power LED (WAN) A-12

### power status (monitoring) 15-19

### Power Supplies LEDs (front panel) A-10

### power thresholds, configuring 3-5

### power, turning off 14-17

### PPP Multilink (MP) 3-2

configuring 3-25

### PPTP

#### configuring

base group 12-6, 12-12  
 group (internal) 12-23, 12-28  
 user (internal server) 12-38, 12-41  
 configuring system-wide parameters 7-2  
 statistics 15-48

### prerequisites, system administrator xxxvii

### protocols, session (monitoring) 15-36

## Q

### quitting the Manager (logout) 1-21

## R

### RADIUS

accounting, configuring 5-11  
 accounting record attributes 5-12  
 Class attribute format to authenticate group name 12-16  
 configuring, authentication server 5-4  
 Funk server 5-2, 12-1

### reboot system 14-17

saves log file 10-6, 14-17, A-1

### redundancy

configuring, system 8-12  
 SEP modules 15-20

### references (bibliography) xxxix

### Refresh (icon) 1-22

- refresh Monitoring screens 14-20
- refreshing screen content 1-22
- regulatory agency notices B-9
- requirements
  - browser 1-1
  - cookies 1-2
  - Internet Explorer 1-1
  - JavaScript 1-1
  - Netscape Navigator 1-1
- RIP 3-1, 3-2
  - configuring on Ethernet interface 3-10
  - configuring on WAN interface 3-18
  - MIB-II statistics 15-85
- root certificates 14-34
- routing table (monitoring) 15-2
- rules 13-1
  - add security association to, on filter 13-36
  - assign to filter (traffic management) 13-34
  - change security association on 13-37
  - filter, configuring 13-9
- rules, NAT, configuring 13-40
  - add 13-42
  - modify 13-42

**S**

- SAs *See* security associations
- save event log 15-6
- Save (icon) 1-21
- Save Needed (icon) 1-21
- SAVELOG.TXT file 10-6, 14-17, A-1
- saving configuration file with CLI 16-7
- screen
  - login 1-3
  - login, using HTTPS 1-17
- SDRAM memory 15-10
- SecurID, configuring authentication server 5-6
- security associations 13-1
  - add to rule on filter 13-36
  - change on rule 13-37
  - configuring 13-19
    - add 13-22
    - delete 13-28
    - modify 13-22
  - default, table 13-21
  - IKE proposals in 13-19
  - negotiation phases 13-19
- SEP modules
  - functions performed 15-20
  - redundancy 15-20
  - status and statistics 15-20
  - used by sessions (monitoring) 15-38
- servers, configuring system access to 5-1
- Session Timeout (error) A-3

- sessions
  - active (administration) 14-3
  - active (monitoring) 15-26
  - count, definition 14-4, 15-26
  - data (monitoring) 15-26
  - detail 14-8, 15-30
    - parameter definitions 14-12, 15-34
  - encryption algorithms used 15-39
  - logout all 14-4
  - maximum permitted 14-5, 15-27
  - parameter definitions 14-7, 15-29
  - protocols (monitoring) 15-36
  - SEP modules used 15-38
  - statistics (administration) 14-3
  - top ten 15-41
    - by data 15-41
    - by duration 15-43
    - by throughput 15-45
- shutdown system 14-17
- SMTP servers, configuring for events 10-18
  - add 10-20
  - modify 10-20
- SNMP
  - configuring internal server 9-7
  - event trap destinations, configuring 10-14
    - add 10-15
    - modify 10-15
  - MIB-II statistics 15-98
  - traps, configuring "well-known" 10-8
- SNMP communities, configuring 9-8
  - add 9-10
  - modify 9-10
- software image
  - filenames 14-15, 15-10
  - update on VPN Concentrator 14-14
  - version info 14-14, 15-10
- speed, configuring Ethernet interface 3-9
- split tunneling, IPSec
  - configuring network list for 12-10, 12-27
  - discussion 12-10
  - requires Mode Configuration 12-9, 12-26
- SSL
  - client authentication 9-12
  - configuring internal server 9-10
  - statistics 15-74
- SSL certificate 9-10, 14-35
  - generating 14-43
  - installing in browser 1-3
  - installing with Internet Explorer 1-4
  - installing with Netscape 1-10
  - viewing with Internet Explorer 1-9
  - viewing with Netscape 1-15
  - VPN Concentrator 1-3
- starting the CLI 16-2

- static routes, configuring for IP routing 8-2
    - add 8-3
    - modify 8-3
  - statistics 15-47
    - accounting 15-68
    - address pools 15-76
    - authentication 15-66
    - DHCP 15-75
    - DNS 15-65
    - events 15-62
    - filtering 15-69
    - HTTP 15-61
    - IPSec 15-55
    - L2TP 15-51
    - MIB-II 15-77
      - ARP table 15-94
      - Ethernet 15-96
      - ICMP 15-92
      - interfaces 15-78
      - IP traffic 15-82
      - OSPF 15-87
      - RIP 15-85
      - SNMP 15-98
      - TCP/UDP 15-80
    - PPTP 15-48
    - sessions (administration) 14-3
    - SSL 15-74
    - synchronous 15-14
    - T1/E1 15-14
    - Telnet 15-63
    - VRRP 15-71
    - WAN 15-14
  - status bar in Manager window 1-19
  - Status LED (SEP) A-11
  - Status LED (WAN) A-12
  - stopping
    - CLI 16-7
    - the Manager (logout) 1-21
    - the VPN Concentrator 14-17
  - strings, text, format xl
  - subnet masks, format xl
  - superuser *See* administrators
  - support, Cisco xli, 1-20
  - Support (tab on Manager screen) 1-20
  - swap configuration files 14-32
  - switchover, automatic (redundancy) 8-12
  - Sync LED (WAN) A-13
  - synchronous statistics 15-14
  - syslog servers, configuring for events 10-16
    - add 10-17
    - modify 10-17
  - system configuration section of Manager 4-1
  - system identification, configuring 11-2
  - System LED A-10
  - system reboot 14-17
  - system shutdown 14-17
  - system status (monitoring) 15-9
- ## T
- T1/E1 3-2
    - line error conditions (WAN card) A-13
    - parameters, configuring on WAN interface 3-23
    - selecting, for WAN interface 3-15
    - statistics 15-14
  - tab (on Manager screen)
    - Administration 1-21
    - Configuration 1-21
    - Help 1-20
    - Logout 1-21
    - Main 1-20
    - Monitoring 1-21
    - Support 1-20
  - table of contents, Manager 1-24
  - TCP/UDP MIB-II statistics 15-80
  - Technical Assistance Center (TAC), contacting 1-21
  - Telnet
    - accessing CLI 16-2
    - configuring internal server 9-6
    - statistics 15-63
  - Telnet over SSL
    - configuring internal server 9-6
    - shareware client 9-6
  - temperature sensors (monitoring) 15-11
  - text strings, format xl
  - TFTP
    - configuring internal server 9-4
    - file transfer 14-32
  - Throughput LED A-10
  - throughput, top ten sessions sorted by 15-45
  - time and date, configuring 11-3
  - time zone, configuring 11-3
  - timeout, administrator 14-28
  - timeslots, configuring WAN 3-24
  - title bar in Manager window 1-19
  - top frame (Manager toolbar) in Manager window 1-20
  - top ten sessions (monitoring) 15-41
  - traffic management, configuring 13-5
  - transmission mode, configuring Ethernet interface 3-9
  - traps, configuring
    - "well-known" 10-8
    - destination systems 10-14, 10-15
    - general events 10-8
    - specific events 10-13
  - troubleshooting A-1
    - consult event log 10-5, 15-4
    - files created for A-1
  - tunnel default gateway, configuring 8-5

- tunneling protocols
  - configuring 7-2
  - section of Manager 7-1
- Tx LED (Ethernet) A-11
- type (model number), system 15-10
- typographic conventions xxxix

## **U**

- understanding the VPN Concentrator Manager window 1-19
- update software on VPN Concentrator 14-14
- usage graph
  - LEDs (monitoring) 15-11
  - LEDs (table) A-11
  - selector button 15-25
- user attributes, default
  - See* base group 12-3
- user management
  - configuring 12-3
  - section of Manager 12-1
- users, configuring on internal server (user management) 12-33
  - add 12-34
  - delete 12-34
  - modify 12-34
- using the CLI 16-3
- using the VPN Concentrator Manager 1-1

## **V**

- viewing SSL certificates
  - with Internet Explorer 1-9
  - with Netscape 1-15
- voltage status 15-19
- VPN Concentrator Manager
  - errors A-2
  - logging in 1-18
  - logging out 1-21
  - navigating 1-24
  - organization of 1-23
  - understanding the window 1-19
  - using 1-1
- VRRP
  - configuring 8-12
  - statistics 15-71

## **W**

- WAN card
  - LED indicators A-12
  - putting in loopback mode A-13
- WAN interface
  - See* interfaces
- wildcard masks 7-15, 7-17, 13-8, 13-16
  - format xl

- window, Manager, understanding 1-19
- Windows 2000 client
  - and Mode Configuration 12-9, 12-27
  - configure transport mode 13-24
  - L2TP over IPSec support 7-1, 12-7, 12-23, 12-39
  - PPTP support 12-6, 12-23, 12-38
- WINS, configuring for group 12-22
- workstations allowed administrator access 14-26

## **X**

- X.509 digital certificates 14-35
- XAuth 12-9, 12-26

## **Y**

- You are using an old browser or have disabled JavaScript (error) A-5